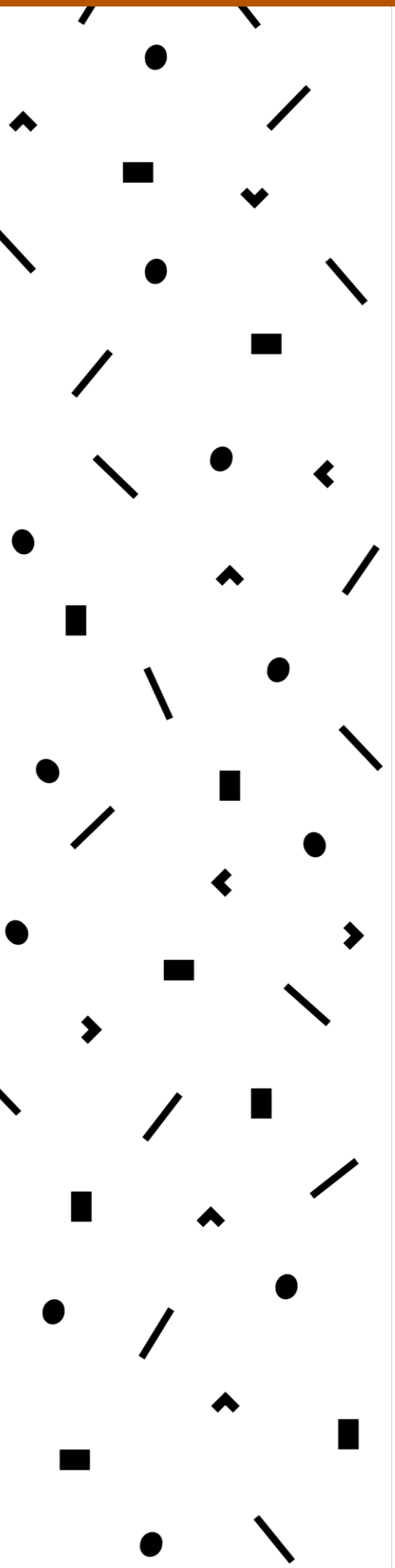


LAMK Lahden ammattikorkeakoulu
Lahti University of Applied Sciences

MPLS-verkon soveltuvuus suojauksen viestiyhteyksiin

LAHDEN
AMMATTIKORKEAKOULU
Tekniikan ala
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka
Opinnäytetyö
Kevät 2017
Jani Kerkkänen

Lahden ammattikorkeakoulu
Tietotekniikan koulutusohjelma

KERKKÄNEN, JANI:

MPLS-verkon soveltuvuus suojauksen viestiyhteyksiin

Tietoliikennetekniikan opinnäytetyö, 39 sivua

Kevät 2017

TIIVISTELMÄ

Opinnäytetyön tavoitteena oli tutkia MPLS-verkon soveltuvuutta suojauksen viestiyhteyksiin Suomen kantaverkossa. Lisäksi työssä pohdittiin, millaisia testejä tulisi MPLS-verkolle tehdä, jotta sen soveltuminen suojauksen viestiyhteyksiin voitaisiin varmistaa ja todentaa.

Suojauksen viestiyhteydet ovat tärkeä osa kantaverkon toimintaa, sillä niitä käytetään verkkoa suojaavien laitteiden välillä jatkuvaan viestintään. Releet välittävät suojauksen viestiyhteyden välityksellä mittaustietoja sekä laukaisusignaaleja toisilleen. Suojauksen viestiyhteyksien avulla suojareleet tekevät luotettavammin ja nopeammin päätöksiä siitä, tarvitseeko verkon jokin osa irrottaa muusta verkosta vikatilanteessa. Vikaantuneen verkon osan irrottaminen estää vikatilanteen laajenemisen.

MPLS eli leimakytkentä on menetelmä, jolla voidaan luoda nopea kytkentäinen tietoverkko reititetyn tai pakettikytkentäisen verkon päälle. MPLS on monipuolinen ja laajalti käytetty verkko. PDH- ja SDH-verkot ovat vanhoja TDM-siirtotekniikoita, joissa kulkuaikaviiveen vaihtelu on todella vähäistä ja siksi TDM-siirtotekniikka soveltuu hyvin viivekriittisiin palveluihin.

MPLS-verkko soveltuu suojauksen viestiyhteyksiin sen monipuolisuuden ja tehokkuuden vuoksi. MPLS ja QoS yhdessä takaavat kriittiselle liikenteelle vaaditun korkean prioriteetin, jotta suojaussignaalit pääsevät varmasti perille. Soveltuvuus varmistetaan erilaisin testein myöhemmin tänä vuonna. MPLS:ää tullaan todennäköisesti käyttämään suojauskäytössä tulevaisuudessa enemmän, kun saadaan tarpeeksi näyttöä sen soveltuvuudesta.

Asiasanat: MPLS, PDH, SDH, telesuojaus, kantaverkko, QoS

Lahti University of Applied Sciences
Degree Programme in Information Technology

KERKKÄNEN, JANI:

MPLS network suitability for teleprotection

Bachelor's Thesis in Telecommunications, 39 pages

Spring 2017

ABSTRACT

This thesis deals with the suitability of the MPLS network for teleprotection in the Finnish power transmission system, and of what kind of tests should be done for the MPLS network to ensure the suitability for teleprotection use.

Teleprotection is an important part of the operation of a transmission system, because they are used between the protection equipment for continuous communication. Teleprotection is used by protective relays to transmit metering data and trip signals. Protective relays use teleprotection to increase the reliability and speed of making the decision whether to disconnect a part of the grid, should a fault happen.

MPLS is a method for creating fast switched network on a routed or packet switched network. The MPLS network is versatile and widely used. PDH and SDH networks are older time-division multiplexing networks in which the propagation time delay variation is minimal and therefore are suitable for very delay critical services.

The MPLS network is suitable for teleprotection because of its versatility and efficiency. MPLS and QoS together ensures high priority for mission critical traffic so the teleprotection signals will certainly go through the network. The suitability will be ensured with various tests later this year. The MPLS network is likely to be used more in teleprotection when there is enough proof of its suitability for such use.

Key words: MPLS, PDH, SDH, teleprotection, power grid, QoS

SISÄLLYS

LYHENNELUETTELO

ADC	Asymmetrical Delay Control, MPLS-verkon priorisointitekniikka, jolla on tarkoitus estää sähköverkon suojauksen virhelaukaisuja
ATM	Asynchronous Transfer Mode, eräs tietoliikenneverkkotekniikka
BER	bit error rate, signaalin virheiden määrän suhde virheettömiin bitteihin
BGP	Border Gateway Protocol, autonomisten järjestelmien väliseen reititykseen tarkoitettu protokolla
CE	Customer Edge, MPLS-palvelussa asiakkaan reititin, joka on yhdistetty palveluntarjoajan MPLS-verkkoon
CES	Circuit Emulation Service, palvelu, jota käytetään yhdistämään TDM-pohjaisia suojausyhteyksiä pakettikytkentäisien verkkojen yli
FEC	Forwarding Equivalence Class, MPLS:n edelleenvälitysluokka, johon kuuluu samalla tavalla kohdeltavat ja välitettävät paketit
GAL	Generic Alert Label, MPLS-verkon komponentti, jota käytetään G-ACh:n merkkaamiseen
IEEE	Institute of Electrical and Electronics Engineers, merkittävä kansainvälinen teknillinen järjestö. Julkaisee laajasti käytettyjä suosituksia
IETF	The Internet Engineering Task Force, organisaatio, joka vastaa IP-standardoinnista
IP	Internet Protocol, pakettien välittämisestä huolehtiva protokolla internetverkoissa
ITU	International Telecommunication Union, kansainvälinen televiestintäliitto
LSP	Label-Switched path, MPLS-verkon ennalta määritetty reitti

LSR	Label switching router, MPLS-verkon reititin, joka välittää paketin käyttäen pakettiin liitettyä leimaa (label)
MPLS	Multiprotocol Label Switching, Leimakytkentä - Monipalveluverkko, joka käyttää leimoja pakettien välittämiseen.
MPLS TE	Multi Protocol Label Switching Traffic Engineering, MPLS-verkon liikenteen ohjaus toiminne, jonka ideana on optimoida verkon liikenne
NMS	Network Management System, verkonhallintajärjestelmä
OAM	Operations, Administration and Maintenance, joukko työkaluja ja tapoja järjestelmän käyttöön ja ylläpitoon
OSI-malli	Open Systems Interconnection Reference Model, tiedonsiirtoprotokollat yhdistävä seitsemänkerroksinen käsitemalli
OSPF	Open Shortest Path First, autonomisen alueen sisäinen reititysprotokolla, joka laskee algoritmin perusteella paketille optimaalisimman reitin TCP/IP-verkossa
PDH	Plesiochronous Digital Hierarchy, ”melkein” synkroninen kanavointitekniikka, jota käytetään tiedonsiirtoon piirikytkentäisessä verkossa
PHP	Penultimate Hop Popping, MPLS-verkon toiminto, jossa poistetaan MPLS-paketin päällimmäinen leima ennen lähettämistä reunareitittemelle
PW	Pseudowire, Näennäisjohdin on palvelu, jonka avulla kuljetetaan siirtoyhteyksiä MPLS-verkon yli.
QoS	Quality of Service, liikenteen luokitteluun ja priorisointiin tarkoitettu tekniikka siirtoverkossa
SDH	Synchronous Digital Hierarchy, tahdistukseen perustuva sykronoidun tiedonsiirron standardi
SPF	Shortest Path First, algoritmi, jota käytetään lyhimmän mahdollisen reitin laskemiseen tietoverkossa

SVY	Suojauksen viestiyhteys, Sähkölinjojen suojausviestien välittämiseen käytettävä viestiyhteys
SyncE	Synchronous Ethernet ITU-T standardi, joka helpottaa kellosignaaleiden kuljettamista tietoverkkojen läpi fyysisellä kerroksella
TDM	Time Division Multiplexing, aikajakoinen yhteyksien lomittelutekniikka
TTL	Time To Live, paketin elinaikaa kuvaava arvo, ilmoitetaan hyppyjen määränä
VoIP	Voice over Internet Protocol, Metodi puheluiden siirtämiseen reaaliajassa esimerkiksi internetin yli
VPN	Virtual Private Network, jaettua alustaa hyödyntävä yksityinen verkko
VRF	Virtual routing and forwarding, teknologia, joka sallii reititystiedon tallentamisen samaan reitittimeen moneen kertaan ilman konflikteja, käytetään Layer 3 VPN:ssä

1 JOHDANTO

Tässä opinnäytetyössä tutkitaan, voiko perinteiset suojauksen viestiyhteydet korvata nykyaikaisemmalla MPLS-tekniikalla. Työssä tutkitaan, täyttääkö MPLS-verkko suojauksen viestiyhteydelle annetut vaatimukset. Lisäksi työssä pohditaan erityisesti, millaisia testejä tulisi MPLS-verkossa tehdä, jotta voitaisiin todeta sen soveltuvuus kriittisiin suojauksen viestiyhteyksiin.

Tässä opinnäytetyössä käydään läpi MPLS-verkon periaatteita, tutustutaan Suomen kantaverkon suojausperiaatteisiin, telesuojauksen periaatteisiin ja relesuojaukseen. Suojauksen viestiyhteyksiä käytetään tiedonsiirtoon eri sähköasemilla olevien suojareleiden välillä. Niitä käytetään välittämään sekä mittaustietoja että releiden mahdollisia laukaisusignaaleja. Fingridin tapauksessa suojauksen viestiyhteyksiin käytettävältä verkolta vaaditaan äärimmäistä toimintavarmuutta, nopeutta ja luotettavuutta, sillä kyseessä on Suomen kantaverkon suojaus.

2 KANTAVERKON SUOJAUS

2.1 Kantaverkko

Kantaverkko on Suomen kattava sähkönsiirtoverkko, joka yhdistää tuotanto- ja kulutuskeskittymät. Kantaverkkoon liittyvät myös kantaverkkoyhtiöiden väliset yhteydet, jotka ylittävät valtion rajat. Kantaverkko on rengaskäyttöinen, eli silmukoitu. 400 kilovoltin (kV) ja 220 kV voimajohtojen ja sähköasemien lisäksi kantaverkkoon kuuluu voimansiirron kannalta keskeisimmät 110 kV:n voimajohdot ja sähköasemat. (Kantaverkkowiki 2017.)

Kantaverkossa sähköä siirretään sähköä tuottavilta voimalaitoksilta kulutusalueille ja teollisuuteen suurkäyttäjille. Näiden lisäksi sähköä siirretään rajasiirtoyhteyksillä Suomeen ja Suomesta naapurimaihin. Pienkuluttajille eli muun muassa asuinrakennuksille sähkö tuodaan alue- ja jakeluverkoista. Kantaverkon toimintavarmuuden tulee olla erinomainen, eikä yksittäisen osan vioittuminen saa keskeyttää sähkönsiirtoa kantaverkossa. Tämä varmistetaan N-1-periaatteella. N-1 -periaate tarkoittaa sitä, että järjestelmän tulee kestää mikä tahansa yksittäinen vika milloin tahansa laajentamatta vian vaikutusaluetta. (Kantaverkkowiki 2017.)

2.2 Siirtoverkon viat

Suomen kantaverkko on rakennettu pääosin avojohdoilla ja siksi altis monille ulkoisille vian aiheuttajille. Vaikka siirtojohdot on pääsääntöisesti suojattu ukkosjohtimilla, valtaosa vioista on salamoiden aiheuttamia. Kantaverkossa suojaudutaan monilta eri vikatyypeiltä. Vikoja ovat esimerkiksi oikosulku, maasulku, johdinkatkos ja ylikuorma. Vikoja aiheuttavat muun muassa seuraavat syyt: ylijännitteet, eristyksen rikkoutuminen, vieras esine johtimien välillä, työntekijöiltä unohtuneet

työvälineet ja virheelliset käyttötoimenpiteet. Vikaantunut verkon osa tulee irrottaa muusta verkosta mahdollisimman nopeasti voimajärjestelmän haittojen minimoimiseksi. Voimajärjestelmään kuuluvat voimalaitokset, kantaverkko, jakeluverkot sekä sähkön kuluttajat. (Kantaverkkowiki 2017.)

2.3 Relesuojaus

Relesuojauksella pyritään irroittamaan vikaantunut osa verkosta ja suojaamaan näin johtoja, muuntajia ja muita verkon osia. Suojareleitä asennetaan sähköasemille suojaussuunnitelman mukaisesti. (Kantaverkkowiki 2017.)

Perusedellytykset relesuojaukselle ovat nopeus, luotettavuus ja selektiivisyys. Nopeudella pyritään minimoimaan vikavirran aiheuttamat vahingot. Pidentynyt vika-aika vaarantaa lisäksi voimajärjestelmän stabiiliuden. (Kantaverkkowiki 2017.)

Luotettavuudella tarkoitetaan sitä, ettei rele laukaise ilman, että sen alueella on vikaa, tai jätä laukaisematta vikatilanteessa. Releen laukaisu on erityisen tärkeää, sillä pääreleen ja varasuojauksen toimimattomuus voi aiheuttaa verkon suurhäiriön. Yksittäisen releen aiheeton laukaisu ei kaada koko verkkoa N-1-periaatteen ansiosta.

Selektiivisyydellä tarkoitetaan sitä, että vian ilmettyä vain vikaa lähimmät katkaisijat avataan. Tällöin vika-alue voidaan rajata ja haitat voimajärjestelmälle minimoida. Suojauksen tulee olla riittävän herkkä ja toimia kaikissa suojausalueen oiko- ja maasulkutilanteissa, vaikka vikavirrat olisivat ennakoitua pienempiä. Suojaus ei saa irrottaa johtoa kuin ennalta määrätyissä vikatapahtumissa. Vikatilanteessa pyritään irrottamaan mahdollisimman pieni osa verkosta. (Kantaverkkowiki 2017.)

2.4 Suojareleet

Suojareleiden toiminta perustuu mittauksiin. Ne havahtuvat ja laukaisevat tarkkailemansa sähkösuureen muutoksista. Suojareleiden tehtävänä on

muodostaa tieto, jonka perusteella virtapiiri katkaistaan tai siitä annetaan hälytys. (Kantaverkkowiki 2017.)

Mittaavat releet ovat normaalitilassa siihen saakka, kunnes releen tarkkaileman suureen arvo poikkeaa sallituista toiminta-arvoista. Suureen poikkeaminen toiminta-arvoista aiheuttaa releen havahtumisen. Jos releen havahtuminen kestää tarpeeksi kauan, rele antaa joko laukaisukäskyn, hälytyksen tai molemmat. (Kantaverkkowiki 2017.)

Yleisimmät käytössä olevat johtosuojareleet ovat:

- distanssirele
- differentiaalirele
- nollavirtarele
- ylivirtareleet
- maasulun suuntarele.

Näistä johtosuojareleistä käsitellään jatkossa vain distanssi- ja differentiaalireleitä. Distanssi- ja differentiaalireleet ovat kantaverkon ainoat johtosuojareleet, joilla käytetään viestiyhteyksiä. (Kantaverkkowiki 2017.)

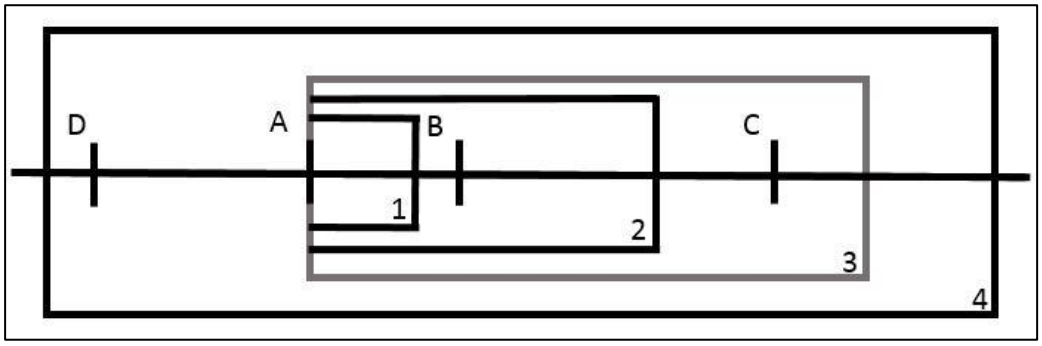
2.4.1 Distanssirele

Kantaverkon johdot ovat lähtökohtaisesti suojattu distanssireleillä. Distanssireleen toiminta perustuu johdon impedanssin laskemiseen mitatusta jännitteestä ja virrasta. Vikatilanteessa tapahtuva impedanssin pieneneminen on helppo mitata, joten se soveltuu hyvin releen toimintaa ohjaavaksi suureeksi. Releen laskemaa impedanssia voidaan käyttää myös vikapaikan etäisyyden arvioimiseen. (Kantaverkkowiki 2017.)

Distanssireleitä on kaksi erilaista tyyppiä: ei-kytkeviä ja havahtuvia. Ei-kytkevä rele mittaa kaikkia vikoja eli kaikkien vaiheiden oiko- ja maasulkuja. Havahtuva rele havahtuu ennen mittauksen aloittamista. Havahtumisen jälkeen rele alkaa mitata vikaa, johon se havahtui. Näistä kahdesta releestä ei-kytkevä rele on nopeampi laukaisemaan.

Kantaverkon nopeimmat releet kykenevät alle 25 millisekunnin laukaisukäskyyn kun hitaammilla vastaava aika on noin 50 - 60 millisekuntia. (Kantaverkkowiki 2017.)

Distanssireleellä toteutettu järjestelmä perustuu vyöhykkeisiin, joilla on jokaisella tietty ulottuma ja hidastus. Kuviossa 1 on esitetty asemalta A asemalle B mittaavan distanssireleen eri laukaisuvyöhykkeet. Kuviossa näkyy yksi voimajohto ja neljä sähköasemaa (A, B, C ja D). Lisäksi kuvioon on piirretty laukaisuvyöhykkeet 1, 2 ja 3 sekä havahtumisvyöhyke 4.



KUVIO 1 Distanssireleen vyöhykkeet

Suurin osa johdosta A-B kuuluu ensimmäiseen vyöhykkeeseen, jotta rele laukaisee mahdollisimman nopeasti ilman hidastuksia. Distanssireleen ensimmäistä vyöhykettä ei voida asettaa kattamaan koko johtoa A-B epätarkkuuksien takia. Tästä syystä vyöhykkeeksi asetellaan reaktanssiarvo, joka kattaa noin 80 - 85 % johdosta A-B. Jotta saadaan koko johdolla esiintyville vioille selektiivinen ja nopea laukaisu, käytetään viestiyhteystoimintoja. Yleisimmät toiminnot ovat salliva aliulottuva toiminto PUTT ja salliva yliulottuva toiminto POTT. Salliva aliulottuva toiminto tarkoittaa viestisignaalin lähettämistä 1.vyöhykkeen laukaisusta. Tällöin vastapään laukaisuehto on yleensä havahtuminen. Salliva yliulottuva

toiminto tarkoittaa viestisignaalin lähettämistä tyypillisesti 2. vyöhykkeen havahtumisesta. Tällöin vastapäässä laukaisuehtona on havahtuminen. Laukaisu tapahtuu, mikäli molemmat releet näkevät vian edessä. Lähettävän releen päässä asetteluna käytetään joko ali- tai yliulottuvaa toimintoa ja vastaanottavan releen päässä aina yliulottuvaa viestiyhteystoimintoa. (Kantaverkkowiki 2017.)

Tyypilliset vyöhykeasettelut ja -ajat:

1. vyöhyke: 85 % johdon pituudesta A-B, ilman hidastusta

2. vyöhyke: vähintään 120% johdosta A-B, hidastus 0,4s > vasta-aseman yli

3. vyöhyke: ulottuma yli johto-osan A-C, hidastus 1 s > koko naapurijohto

4. vyöhyke, havahtumisvyöhyke: ulottuma eteenpäin yli kolmannen vyöhykkeen, taaksepäin ulottuma vaihtelee, t=3-4 s. (Kantaverkkowiki 2017)

Hidastuksella tarkoitetaan releen toiminta-ajan pidentämistä asettelemalla releeseen haluttu viive. Tällä saadaan määrättyä laukaisun nopeus eri paikoissa. (Suojauksen viestiyhteydet 2014.)

Distanssireleiden välisen viestiyhteyden tulee toimia aina, jotta releet toimisivat tarkoituksen mukaisesti. Releet käyttävät viestiyhteyttä mittaustietojen välittämiseen toisilleen. Johdon eri päiden releiden välisellä viestiyhteydellä voidaan varmistaa koko johdolle nopea suojaus myös tilanteissa, joissa vika sijaitsee lähellä johdon päätä. Suojauksen viestiyhteyden merkityksestä distanssisuojaukselle on kirjoitettu enemmän luvussa 4.

2.4.2 Differentiaalirele

Differentiaalireleen toiminta perustuu suojattavan kohteen asetusarvoon ja siihen tulevien virtojen summaan. Rele laukaisee, jos siihen tulevien virtojen summa on suurempi, kuin aseteltu. Differentiaalireleellä suojataan vain se virtamuuntajien välinen alue, jonka virtoja vertaillaan. Differentiaalireleen laukaisunopeus on 30 millisekuntia, eikä siihen aseteta viivettä. (Kantaverkkowiki 2017.)

Differentiaalisuojausta käytettäessä tarvitaan releiden välille viestiyhteys. Viestiyhteys voi olla joko suora optinen kuitu tai viestiverkko, jonka läpi yhteys kulkee. Viestiverkkoa käytettäessä tulee olla tapa, jolla vastapuolen suojarele voi tunnistaa viestisignaalin oikeaksi, jotta vältytään väärien pulssien aiheuttamilta mahdollisilta virhetoiminnoilta.

Differentiaalisuojareleillä toteutetut suojaukset perustuvat Suomen kantaverkossa pääasiassa symmetriseen viiveeseen kumpaankin siirtosuuntaan (niin sanottu "Echo-moodi"). Tällöin johdon eri päissä tehdyt mittaukset voidaan kohdistaa samalle ajanhetkelle ilman ulkoista kelloa. Kulkuajan muuttuminen voidaan tulkita vaihesiirtona mitattavien virtojen välillä ja aiheuttaa releen turhan laukaisun. Kulkuajan muuttumista voi aiheuttaa uudelleenreititys tai viiveen vaihtelu ensisijaisella siirtotiellä. Differentiaalirelettä käyttäessä 1 ms ero todellisen ja laskennassa käytetyn kulkuajan välillä voi aiheuttaa jopa 30 % eron mitattavien virtojen huippuarvoissa. (Suojauksen viestiyhteydet 2014; Line Protection - Johtosuojaus 2013.)

Mikäli viestiyhteys differentiaalireleiden välillä virheilee, se voi aiheuttaa väärän laukaisun. Jos taas viestiyhteys katkeaa, se ei laukaise relettä vaan lukitsee sen. Tässä tapauksessa rele ei ole käytettävissä ja suojauksesta vastaa varasuojaus. (Communication Networks for Smart Grids 2014.)

3 LEIMAKYTKENTÄ (MPLS)

Leimakytkentä (MPLS, Multi Protocol Label Switching) on menetelmä, jolla on mahdollista luoda nopea kytkentäinen verkko valmiiksi reititetyn tai pakettikytkentäisen verkon päälle. MPLS-verkossa pakettien kytkemiseen käytetään leimoja (label). MPLS-tekniikkaa voidaan käyttää kuljettamaan monentyyppistä liikennettä, mutta sitä käytetään pääasiassa IP-liikenteen välittämiseen. MPLS-palveluita voidaan käyttää esimerkiksi yhdistämään useita eri asiakasverkkoja toisiinsa ja toisaalta varmistamaan parempi suorituskyky pienen viiveen vaativalle liikenteelle, kuten puheluille (VoIP). (IEEE 2013.)

MPLS:stä on olemassa kaksi päätoteutustapaa, IP-hallintatason päällä toimiva IP/MPLS ja ohjaus- ja hallintatason yhdistävä MPLS-TP. IP/MPLS on näistä kahdesta käytetympi. Käsiteltävät asiat koskevat sekä IP/MPLS:ää että MPLS-TP:tä, ellei erikseen mainita.

MPLS-menetelmä yhdistää OSI-mallin kerrokset 2 ja 3, minkä ansiosta kytkentätietojen luku ja kirjoitus voidaan tehdä laitteistotasolla ohjelmistotason sijaan. Kytkentätietojen luku laitteistotasolla mahdollistaa nopeamman ja tehokkaamman pakettien välityksen. Kuviossa 2 on esitetty OSI-malli ja sen eri kerrokset. (IEEE 2013.)

KUVIO 2 OSI-malli

3.1 Leimakytkennän hallintataso IP/MPLS-verkoissa

IP/MPLS-verkon hallintataso on toteutettu joukolla protokollia, jotka auttavat kytkentätason määrittelyssä. Hallintatason pääkomponentit ovat reititysprotokollat, reititystaulu, leimojenlevitysprotokollat ja muut signalointiprotokollat, joita käytetään kytkentätason provisiointiin. Hallintatason tärkemmät tehtävät ovat muiden reitittimien löytäminen ja leimapolkujen luonti, eli luoda ja täyttää tietokanta kytkentätiedoille. Reititystiedot sisältävä tietokanta on nimeltään RIB (Routing Information Base), leimat sisältävä vastaava tietokanta LIB (Label Information Base) ja näistä reititin muodostaa kytkentätaulukot (FIB, Forwarding Information Base ja LFIB, Label Forwarding Instance Base), joiden perusteella reititin päättää, kuinka saapuva paketti käsitellään. (IEEE 2013.)

MPLS-verkon kaksi tärkeintä leimojenlevitysprotokollaa ovat LDP (Label Distribution Protocol) ja RSVP (Resource Reservation Protocol). LDP:tä voidaan käyttää signaloimaan automaattisesti leimapolut kaikille verkossa reititetyille IP-osoitteille, kuten MPLS-reitittimille. LDP muodostaa leimatietokannan LIB (Label Information Base), joka sisältää kaikki naapurireitittimiltä vastaanotetut sekä oman reitittimen käyttämät leimat ja näitä vastaavat kohde-IP-osoitteet. RSVP on MPLS-verkon liikenteenhallinnassa käytettävä protokolla tunnelien signalointiin. RSVP:tä voidaan käyttää signaloimaan tietyn QoS-palvelutason leimakytketty polku tietylle sovellukselle tai datavirralle. RSVP:llä voidaan signaloida polun luonti läpi koko MPLS-verkon, jotta vaadittu QoS-palvelutaso olisi taattu koko matkan. (IEEE 2013.)

3.2 Kytkentätason toiminta

IP-verkossa paketin lähettäjä lisää pakettiin vastaanottajan osoitteen. Paketti välitetään lähimmälle reitittimelle, minkä jälkeen paketin vastaanottanut reititin tutkii vastaanottajan osoitteen ja omien

reititystaulujen perusteella, mille reitittimelle paketti tulisi välittää. Jokainen matkalla oleva reititin tekee samat toimet. (Nanog 2016.)

MPLS-verkossa paketin saapuessa verkon reunareitittimelle siihen liitetään kiinteän pituinen leima, joka etukäteen luodun kytkentätaulukon avulla kertoo reitittimelle paketin seuraavan hypyn ja näin hyppy kerrallaan kuljettavan reitin. Toisin kuin perinteisissä IP-verkoissa, MPLS:ssä ei lueta paketin lähettäjän määrittämää vastaanottajan osoitetta jokaisella reitittimellä, vaan pelkästään paketin otsikon MPLS-leima. Ennalta määrättyjen polkujen ja leimojen avulla paketin välittäminen on yksinkertaisempaa ja nopeampaa, kuin vaihtuvanmittaista kohde-IP-osoitteen verkko-osaa tutkimalla. MPLS-verkon ennalta määrättyjen reittien ansiosta voidaan hallita yhteyksien käytössä olevaa siirtonopeutta ja laatua. (Nanog 2016.)

3.3 Leimat ja toiminnot

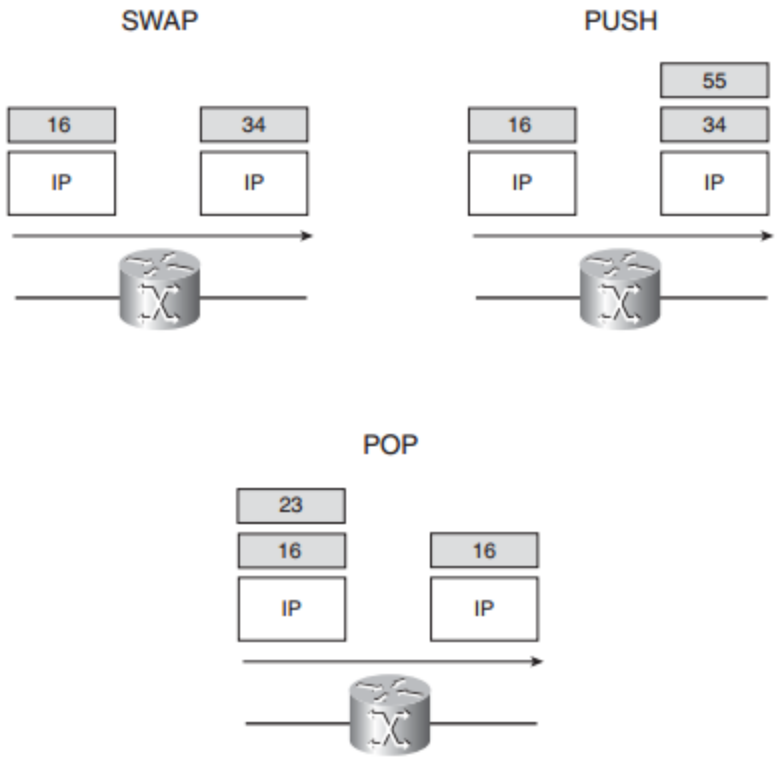
Leima on lyhyt tunniste, jota käytetään pakettien välittämiseen. Paketilla voi olla myös useampi leima päällekkäin, jolloin muodostuu leimapinoja, joita hyödynnetään esimerkiksi VPN-palveluissa.

Leimaa käytetään FEC:n (Forwarding Equivalence Class) tunnistamiseen, joka puolestaan kertoo, mihin paketti välitetään. FEC on joukko samalla tavalla ja samaa reittiä välitettäviä paketteja. Lisäksi leimoja voidaan käyttää esimerkiksi VPN-palvelun tunnistamiseen, uudelleenreititykseen tai OAM-toiminteisiin. (Cisco 2016.)

3.3.1 Operaatiot

MPLS-verkossa leimojen asettamis- ja vaihtamisprosessissa on käytössä kolme operaatiota: push, pop ja swap. Push tarkoittaa leiman asettamista paketille, eli push-operaatiota käytetään esimerkiksi, kun paketti välitetään MPLS-verkkoon. Jos paketilla on ennestään leima ja sille suoritetaan push-operaatio, siirtyvät aiemmat leimat pinossa alaspäin ja uudesta leimasta tulee pinon päällimmäinen. Swap-operaatiota käytetään leiman

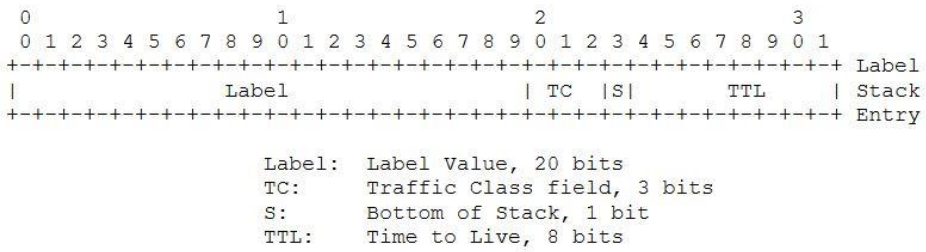
korvaamiseen ulosmenoportin ja ulosmenoleiman perusteella. Kyseinen operaatio siis vaihtaa leiman lisäämättä uutta. Pop-operaatiolla poistetaan paketilta leimapinon päällimmäinen leima. Tämän jälkeen paketin käsittely tehdään paljastuvan leiman tai IP-otsikon perusteella. Jos alta paljastuu esimerkiksi VPN-palveluleima, käsitellään pakettia VPN-palvelun sääntöjen mukaisesti. Kuviossa 3 havainnollistetaan leimaoperaatioita MPLS-verkossa. (Juniper 2016.)



KUVIO 3 MPLS-verkon leimaoperaatiot (Cisco Operations on Labels 2017)

3.3.2 Leiman rakenne

Leimaotsake (MPLS Shim header) on leimakytkentäisessä verkossa pakettiin liitetty 32-bittinen kytkentätieto (kuvio 4). Sen ensimmäiset 20 bittiä ovat leiman arvo, joka voi olla välillä 0-1048575. Ensimmäiset 256 arvoa niistä ovat kuitenkin varattuja. Seuraavia kolmea bittiä kutsutaan Traffic Class -biteiksi, jotka ovat käytössä liikenteen luokitteluun ja priorisointiin (Quality of Service). Seuraava bitti on leimapinon pohja (Bottom of Stack) ja tämän bitin arvo on 0 niin kauan, kunnes se on viimeinen leima leimapinossa. Muutoin bitin arvoksi tulee 1. Loput 8 bittiä ovat TTL-bittejä (Time to Live), jotka määrittävät hyppyjen maksimimäärän. (Cisco 2016.)



KUVIO 4 MPLS-leiman rakenne (IETF MPLS TC Field Definition 2017)

3.4 Leimakytkentäiset reitittimet

MPLS-verkko koostuu LSR-reitittimistä ja LSP:stä (Label Switched Path), eli ennalta määrätyistä poluista. LSR tarkoittaa reititintä, joka tukee MPLS-kehyksiä, MPLS-leimoja ja leimattujen pakettien lähettämistä sekä vastaanottamista. MPLS-verkossa on kolme erilaista LSR-reititintä:

- Ingress LSR on se reititin, joka vastaanottaa paketin MPLS-verkkoon. Ingress LSR lisää paketille leimapinon päällimmäisen

leiman ja välittää eteenpäin. Ingress LSR:ää kutsutaan palvelun näkökulmasta myös PE (Provider Edge) -reitittimeksi. Jos PE liittää paketin johonkin palveluun, esimerkiksi virtuaaliverkkoon (VPN), lisää se pakettiin myös tähän liittyvän leiman.

- Egress LSR on reititin, jonka kautta paketti poistuu MPLS-verkosta. Egress LSR:ää kutsutaan Ingress LSR:n tapaan palvelun näkökulmasta myös PE-reitittimeksi.

- Intermediate LSR on reititin, joka vastaanottaa leimattuja paketteja, suorittaa pop, push tai swap-operaation ja välittää paketin edelleen. Palvelun näkökulmasta Intermediate LSR:ää kutsutaan myös P-reitittimeksi. (Metaswitch Networks 2001.)

3.5 MPLS-verkon lisätoiminteita

MPLS-verkossa on erilaisia lisätoiminteita, joilla verkon laatua ja varmuutta voidaan parantaa. Näitä ovat esimerkiksi liikenteen hallintaan tarkoitettu MPLS-TE, palvelun laadun määrittämiseen käytettävä QoS, erilaiset jonoutumiseen ja ruuhkautumiseen liittyvät liikenteenhallintamekanismit ja yhteyden valvontaan tarvittavat toiminteet.

3.5.1 Liikenteen hallinta IP/MPLS-verkossa (MPLS-TE)

MPLS-TE eli MPLS Traffic Engineering -tekniikan ideana on hallita MPLS-verkon sisällä kulkevaa liikennettä tarkemmin kuin IP-verkossa. MPLS-TE lisää link-state-reititysprokollien tietokantaan perinteisten metriikka-arvojen lisäksi muitakin attribuutteja. Reitti lasketaan tästä TE-informaation tietokannasta saatavien tietojen perusteella käyttäen esimerkiksi SPF (Shortest Path First) -algoritmia. MPLS-TE lisää niihin ehtoja (esimerkiksi reitti, jolla on vaadittu kaista käytettävissä). Lasketun reitin perusteella reititin signaloi RSVP-TE-protokollan avulla leimakytketyn polun. Reititin hyödyntää näitä polkuja palvelun ja verkon tarpeiden mukaisesti. (Cisco 2007.)

Yksi liikenteenhallinan pääkäyttötarkoituksista on verkon kaistakapasiteetin maksimointi. Toinen liikenteenhallinnan käyttötarkoitus on pakottaa liikenne kulkemaan tiettyä reittiä, jolloin sille voidaan taata esimerkiksi vakioviive. Liikenteenhallinta voi mahdollistaa lisäksi liikenteelle aina taatun kaistan. MPLS-TE on usein käytössä tilanteissa, joissa liikenne MPLS-verkossa on suurta, ja verkkolaitteita on paljon. (Cisco 2007.)

3.5.2 Palvelun laatu (QoS)

Palvelun laatu (QoS, Quality of Service) on pääasiassa liikenteen priorisointiin tarkoitettu toiminne. MPLS ei määrittele omia QoS-arkkitehtuureita vaan hyödyntää IP-verkoille määriteltyjä. QoS:n avulla on mahdollista määritellä tärkeälle liikenteelle korkeampi prioriteetti, jotta paketit pääsevät varmasti perille. MPLS-verkoissa QoS on mahdollista toteuttaa kahdella eri tavalla: Integrated Services (IntServ) ja Differentiated Services (DiffServ). IntServ on niin sanotusti ”Hard QoS”, joka mahdollistaa tarkat kaistanleveysvaraukset, jotka tulee konfiguroida polun jokaiseen reitittimeen erikseen. IntServ tarvitsee signalointiprotokollan ja näiden vuoksi on näistä kahdesta huonommin skaalautuva. Näistä kahdesta DiffServ on suositumpi, sillä DiffServ on paremmin skaalautuva eikä tarvitse signalointiprokollaa. DiffServ käyttää MPLS-otsikon TC-bittejä paketin prioriteettiluokan määrittämiseen. Näiden bittien avulla reititin suorittaa tarvittavat toimenpiteet pakettien arvojärjestyksen määrittämiseksi. (Cisco 1999.)

DiffServ mahdollistaa kolme eri tunnelointitilaa, Uniform, Pipe ja Short-Pipe. Tunnelointitilat mahdollistavat verkon palvelun laadun hallinnan MPLS-verkon MPLS-paketeille. Tunnelointitilat määrittävät LSR:n suorittamat toimenpiteet paketeille, joilla on verkkoon saapuessaan tai verkosta poistuttaessa ennestään jokin PHB (Per Hop Behaviour)-merkintä. (Cisco 1999.)

3.5.3 Liikenteenhallintamekanismit

Pakettiverkkojen kehityksen myötä syntyi tarve kehittää sopivia liikenteenhallintamekanismeja. QoS:n toiminta perustuu siis erilaisiin liikenteenhallintamekanismeihin. Näitä mekanismeja ovat liikenteen luokittelu, liikenteen merkkaus, käsittelysääntöjen määrittely, liikenteen muotoilu, ruuhkanhallinta, jononhallinta sekä linkin hajauttaminen ja lomittaminen. Nämä mekanismit auttavat välttämään ja hallitsemaan verkon ruuhkautumista. (Alvarez 2006, 31.)

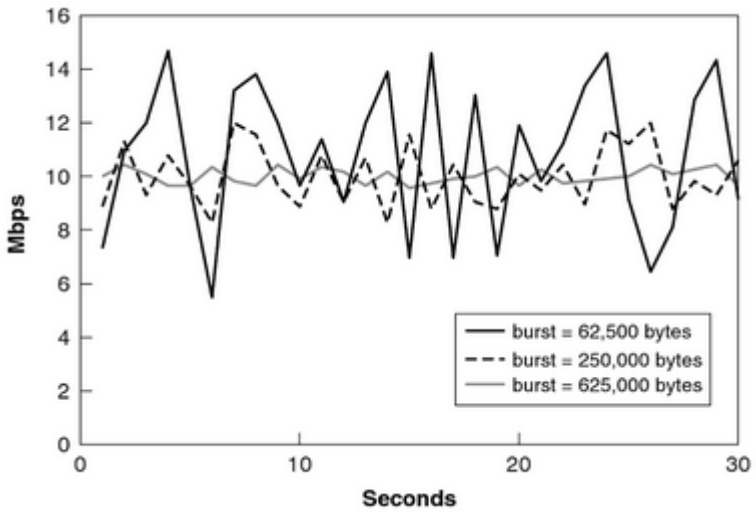
DiffServ QoS vaatii liikenteen identifioinnin ja sen jälkeen luokittelun ryhmiin. Lisäksi DiffServ vaatii sääntöjen määrittämisen kuvaamaan luokitellun liikenteen käyttäytymisen jokaisella hypyllä (PHB). Luokittelu on prosessi, joka valitsee merkattavan liikenteen. DiffServin tapauksessa liikennettä voidaan luokitella joko MF- (Multi Field) tai BA (Behaviour Aggregate) -tunnisteen avulla. DiffServ käyttää liikenteen luokittelua tarjotakseen eritasoista palvelua eri luokille. Liikenne voidaan luokitella käytettävästä verkosta riippuen seuraavin kriteerein:

- sovelluksen tyyppi
- lähde- tai kohde-IP-osoite
- saapuvan liikenteen liityntä
- class of Service (CoS) -arvo Ethernet-otsikossa
- type of Service (ToS) -arvo IP-otsikossa
- MPLS Traffic Class (TC) -arvo MPLS-leimassa.

MPLS-pakettien merkkauksessa käytettäviä MPLS-leiman TC-bittejä on kolme. Niitä käytetään sekä PHB:n että hylkäämisprioriteetin määrittämiseen. IP-liikenteen luokitteluun käytetään IP-otsikon kuutta DiffServ-bittiä, jotka kertovat paketin DSCP:n (DiffServ Codepoint). Reitittimet lukevat jokaisella hypyllä otsikon DSCP:n, jonka avulla päättävät, mikä paketti saa mennä ensin. Välittäessä IP-liikennettä MPLS-verkossa, oletuksena kolme merkittävintä DSCP:n kuudesta bitistä kopioidaan MPLS:n TC-kenttään, jonka perusteella prioriteetti luetaan välittäessä liikennettä MPLS-verkossa. TC-kentän arvon perusteella

ajoitusmekanismi takaa liikenteelle tarvittavan kaistan ja prioriteetin. (Cisco 1999.)

Liikenteen käsittelysääntöjä (Traffic Policing) käytetään liikennemäärän hallintaan. Näitä sääntöjä käytettäessä tietyn solmun liikennemäärä mitataan ja verrataan ennalta määritettyyn liikenneprofiiliin. Vertailun tuloksia käytetään päättämään, välitetäänkö, merkataanko vai hylätäänkö paketti. Liikenneprofiilin kuvaamiseen käytetään merkkisäiliötä (Token bucket). Merkkisäiliöllä on kaksi parametria: merkkivirran nopeus ja säiliön koko. Merkkivirran nopeus määrittää, millä taajuudella uusi merkki saapuu. Säiliön toimintaperiaate on yksinkertainen: säiliöön lisätään jatkuvasti merkkejä tietyllä taajuudella. Paketin saapuessa reitittimelle tarkistetaan, onko säiliössä paketin verran merkkejä. Jos säiliössä on paketin verran tai enemmän merkkejä, poistetaan merkki säiliöstä ja suoritetaan ennalta määrätty toimenpide. Jos säiliössä on vähemmän merkkejä, suoritetaan vaihtoehtoinen toimenpide. Kuviossa 5 esitetään kolme eri liikennevirtaa samalla 10 Mbps nopeudella, mutta eri liikenneprofiililla. (Alvarez 2006, 32.)



KUVIO 5 10 Mbit/s liikennevirrat eri liikenneprofiileilla (Alvarez 2006, 33)

Liikenteen muotoilu (Traffic Shaping) on toinen usein käytetty mekanismi liikennemäärän hallintaan. Liikenteen muotoilun toiminta on samankaltainen liikenteen käsittelysääntöjen kanssa. Liikennettä mitataan ja verrataan liikenneprofiiliin. Muotoilu vaatii kuitenkin puskurin tai jonon paketeille, jotka ylittävät profiilin. Muotoilun avulla solmun on mahdollista ottaa vastaan liikennepurskeita ja tasoittaa näitä välittämällä eteenpäin määrätyn profiilin mukaisesti. (Alvarez 2006, 35, 36.)

Ruuhkanhallinnan kaksi suosittua mekanismia ovat puskurin allokointi ja liikenteen muotoilu. Kun verkossa ilmenee ruuhkaa, liikennettä hallitaan jonolla tai puskurilla. Jonoja voi olla useampi kuin yksi. Liikenteen jonoutuessa reititin päättää, kuinka jono puretaan eli mikä paketti välitetään seuraavaksi. Jokaiselle jonolle voidaan varata tietty määrä puskuria tai kaistanleveyttä. Näin voidaan vaikuttaa tietyn jonon viiveeseen, viiveen vaihteluun ja pakettien häviöön. (Alvarez 2006, 37.)

Yksinkertainen lähestymistapa ruuhkanhallintaan on käyttää yhtä jonoa first-in, first-out (FIFO) -menetelmällä, eli jonoon saapuneet paketit välitetään saapumisjärjestyksessä. Jonolla on tietty puskuri, jonka täyttyessä reititin alkaa hylkäämään saapuvia uusia paketteja, kunnes puskuriin tulee tilaa. Tätä kutsutaan tail drop -menetelmäksi. (Alvarez 2006, 37.)

Aktiiviseen jonon hallintaan on kaksi usein käytettyä mekanismia: RED (Random early detection) ja WRED (Weighted random early detection). RED on mekanismi, joka sallii puskurin täyttymisen tiettyyn rajaan asti, jonka jälkeen paketteja pudotetaan satunnaisesti. Jos pakettien määrä saavuttaa ylärajan raja-arvon, kaikki paketit pudotetaan. WRED on kuin RED, mutta hyödyntää pakettien pudottamisessa lisäksi paketin merkkauksen painoarvoa. WRED osaa ottaa huomioon esimerkiksi paketin CoS-arvon. Esimerkkinä tietyille CoS-arvoille voidaan asettaa raja-arvoksi 30%, jolloin kyseisiä paketteja aletaan pudottaa, kun 30% puskurista on käytetty. (Alvarez 2006, 40, 41.)

Hyvä esimerkki QoS:n tarpeesta on verkko, jossa käytetään paljon VoIP eli Voice over IP -palveluita. VoIP-paketit tulee toimittaa perille tietyssä ajassa, tai paketit vanhenevat ja siksi ne täytyy asettaa korkeimmalla prioriteetillä kulkevaksi liikenteeksi. (Cisco 1999.)

3.6 Leimakytkentäverkon yhteydenvalvontatoiminteita

MPLS OAM ja survivability on tarkoitettu toiminnoiksi, joilla pyritään vähentämään verkon hallintaan ja valvontaan liittyvää käytön monimutkaisuutta. Yksi OAM:n tavoitteista on tarjota tarvittavat työkalut verkonvalvontaan ja hallintaan samoilla ominaisuuksilla, kuin aiemmilla siirtotavoilla. OAM sisältää kaikki pseudowiren (PW) tai LSP:n eheyden varmistamiseen tarkoitetut työkalut. OAM on esimerkiksi suunniteltu kulkemaan samaa reittiä, kuin data, jolloin se valvoo pseudowirea tai LSP:tä.

Kaksi OAM:n mekanismien tärkeää komponenttia ovat G-ACh (Generic Associated Channel) ja GAL (Generic Alert Label). Nämä kaksi komponenttia mahdollistavat käyttäjän lähettää mitä tahansa hallintaliikennettä pseudowiren tai LSP:n yli. G-ACh on kuin oma kanava pseudowiressa ja kuljettaa OAM-vestejä. (IETF 2011.)

3.7 MPLS-verkon palveluita

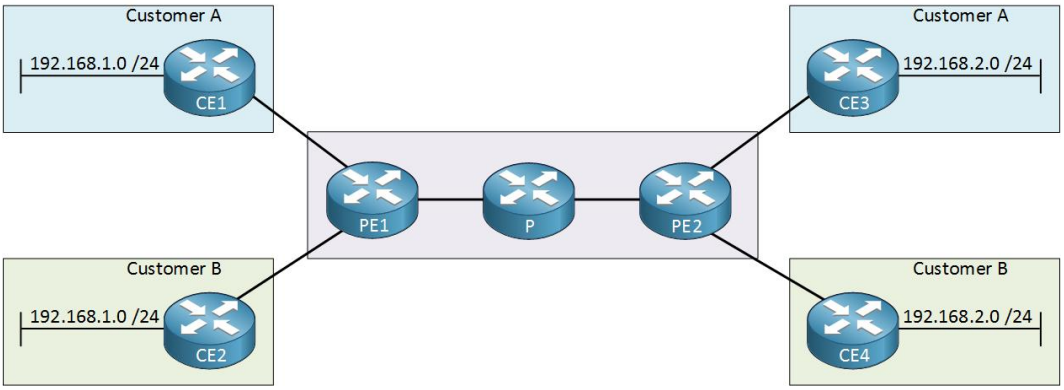
3.7.1 Virtuaaliverkot

Virtuaaliverkko (VPN, Virtual Private Network) on tiedonsiirtoverkko, jossa yhteydet on toteutettu käyttäen jaettua infrastruktuuria ja jolla on samat pääsy- ja turvallisuuskäytännöt kuin yksityisellä verkolla. MPLS-VPN muodostaa jaettuun verkkoon suljetun verkon, jonka yhteydet on tunneloitu leimakytkentää käyttäen. VPN-palvelu voidaan toteuttaa MPLS-verkossa usealla eri tavalla ja MPLS-VPN:t voidaan jakaa sekä Layer 2- että Layer 3 -palveluihin. (TechTarget 2011.)

IP-liikenteelle L3-VPN on näistä kahdesta paremmin skaalautuva vaihtoehto, sillä L3-VPN:ää käyttäessä asiakas ja operaattori molemmat osallistuvat liikenteen reititykseen. Asiakkaan verkon eri osat on yhdistetty operaattorin runkoverkkoon, ja ne käyttävät esimerkiksi OSPF-, EIGRP- tai BGP-reititysprotokollaa, jotta reitit voidaan jakaa asiakkaan muille sijainneille. (Networklessons 2017.)

L3 -VPN verkossa reititys tapahtuu palveluntarjoajan reitittimillä. Palveluntarjoajan reitittimet reitittävät ja välittävät VPN-liikenteen siirtoverkon sisään- ja ulostulopisteissä. L3-VPN tarvitsee toimiakseen tiedot asiakkaan IP-osoitteista. Tietoja käytetään jakamaan ja suodattamaan reittejä virtuaaliverkon sisällä. (TechTarget 2011.)

L3-VPN vaatii enemmän laskentatehoa PE-reitittimiltä kuin Layer 2 VPN, koska Layer 3 reititystaulut ovat asiakkaan verkkojen hallitsemisen vuoksi isompia. Kuviossa 6 näkyy L3-VPN toteutus, jossa on yhdistetty kahden eri toimijan eri toimipaikkojen verkot. (TechTarget 2011.)



KUVIO 6 Esimerkki VPN-toteutuksesta

VPN-liikenteen ei tarvitse olla IP-liikennettä. L2-VPN tarkoittaa liikenteen välittämistä CE-laitteelta (esimerkiksi kytkimeltä tai reitittimeltä) PE-reitittimelle Layer 2 -muodossa, minkä jälkeen liikenne kulkee palveluntarjoajan MPLS-verkon yli. MPLS-verkon jälkeen jälkeen liikenne muutetaan takaisin layer 2 -muotoon. (Juniper 2013.)

L2-VPN:ää käytettäessä reititys tapahtuu asiakkaan kytkimillä, tyypillisesti CE-reitittimillä. Palveluntarjoajan layer 2 VPN:ään yhdistetyn CE-reitittimen tulee valita sopiva VPN-tunneli, jota pitkin liikenteen lähettää. Liikenteen vastaanottava PE-reititin lähettää liikenteen palveluntarjoajan PE-kytkimelle, joka on yhdistetty vastaanottavan pään verkkoon. PE-reitittimet eivät tallenna tai käsittele asiakkaan reittejä, vaan kytkimet on määriteltävä käyttämään oikeaa VPN-tunnelia. (Juniper 2013.)

Muun kuin IP-liikenteen välittämiseen voidaan käyttää esimerkiksi VPWS:ää (Virtual Private Wire Service). VPWS mahdollistaa virtuaalisen point-to-point VPN:n päälle luodun pseudowiren MPLS-verkossa. VPWS yhdistää siis kaksi päätepistettä tai laitetta MPLS-verkon läpi. Tätä voidaan käyttää esimerkiksi frame relay tai TDM-liikenteen välittämiseen MPLS-verkon läpi. (IETF 2006.)

3.7.2 Virtuaalijohdin

Pseudowire eli virtuaalijohdin on palvelu, jonka avulla on mahdollista kuljettaa layer 2 -yhteyksiä MPLS-verkon yli. Pseudowire on linkkitason (layer 2) tunneli. Pseudowire hallitsee liikenteen paketoinnin siirtotielle, ajoituksen, huolehtii järjestystä ja muita toimintoja, jotta pseudowire olisi läpinäkyvä sitä käyttäville. Pseudowireen lähetettävä liikenne paketoidaan MPLS-verkkoon ja verkosta poistuttaessa puretaan ja välitetään takaisin palvelun haluamaan muotoon. TDM-signaalien osalta myös ajoitustieto uudelleengeneroidaan, sillä pakettiverkot eivät toimi aikajakoisesti kuten TDM-verkot. Tuloksena on siis läpinäkyvästi siirretty liikenne reaaliajassa ilman vääristymiä. Pseudowire mahdollistaa esimerkiksi seuraavat liikennöintitavat:

- ATM AAL5 over MPLS
- ATM Cell Relay over MPLS
- Ethernet over MPLS
- Frame Relay over MPLS
- PPP over MPLS
- HDLC over MPLS

- Circuit Emulation Service
- SAToP

(Cisco 2005.)

Näistä suojaskäyttöön tärkeimmät ovat CES (Circuit Emulation Service) ja SAToP (Structure-Agnostic TDM over Packet).

MPLS-verkossa voidaan käyttää CES:iä yhdistämään perinteiset suojausmenetelmät pakettikytkentäisen verkon yli. CES on suunniteltu tukemaan suojausyhteyksiä torjumalla viiveen vaihtelua ja pienentämällä kokonaiskulkuaikaa. Pseudowire on kaksisuuntainen, toisin kuin perinteinen MPLS:n LSP. Pseudowire on niin sanotusti VPN-arkkitehtuurin laajennus. (Nokia 2016.)

SAToP on tapa kapsuloida rakenteettomia TDM-bittivirtoja, esimerkiksi E1, näennäisjohtimina pakettikytkentäisen verkon yli. SAToP ei ota kantaa TDM-rakenteisiin, esimerkiksi kehystykseen, vaan siirtää kaiken saamansa tiedon bittivirtana. Tämä mahdollistaa siirron hyvän hyötysuhteen.

Pseudowiren käyttäminen TDM-liikenteen välittämiseen tuo mukanaan erilaisia haasteita. TDM-liikenne tulee olla paketoitu ja kapseloitu ennen lähettämistä pakettiverkkoon. Pakettiverkot aiheuttavat tiedonsiirtoon ylimääräistä viivettä ja viiveen vaihtelua, joka täytyy poistaa TDM-liikennettä siirrettäessä tasaisen virran saavuttamiseksi. Tästä lisää luvussa 5 ja kuviossa 14.

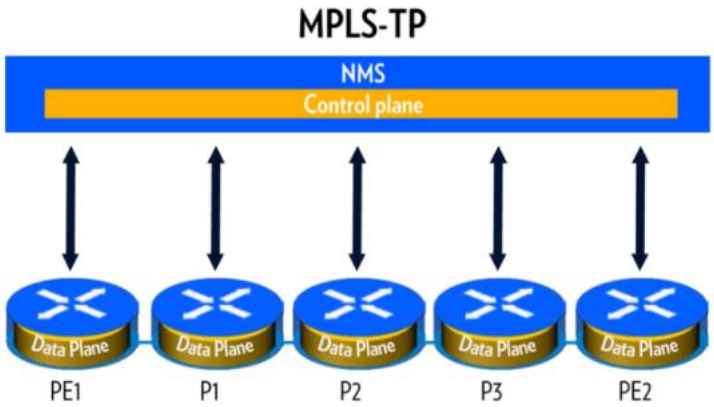
3.8 MPLS Transport Profile (MPLS-TP)

MPLS-TP eli Transport Profile on joukko IETF:n määrittelemiä MPLS-protokollia. MPLS-TP on yksinkertaistettu MPLS, josta on poistettu osa MPLS-toiminnoista, kuten esimerkiksi Penultimate Hop Popping (PHP), LSP:ien yhdistäminen ja Equal Cost Multi Path (ECMP). Kuviossa 7 näkyy

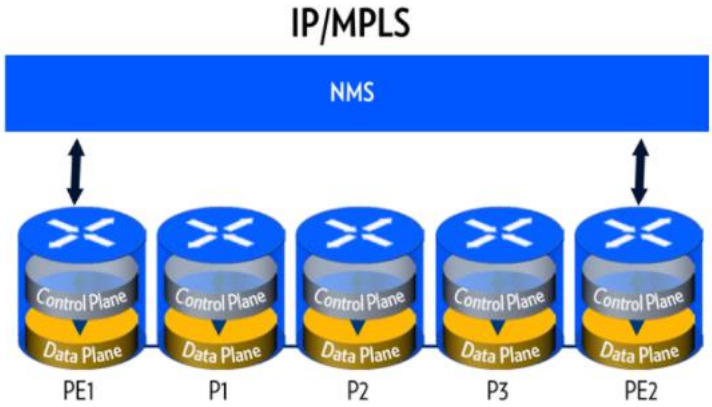
havainnollistava kuvio IP/MPLS:n ja MPLS-TP:n suhteesta. MPLS-TP tarjoaa yhteydellisen siirtotavan paketti- ja TDM-pohjaisille palveluille hyödyntäen jo laajalti käytössä olevaa MPLS-tekniikkaa. Avain tähän on OAM:n (Operations, Administration and Maintenance) ja häiriönsietokykyominaisuuksien määrittely ja toteuttaminen, joilla voidaan tarjota operaattoritason siirtoverkko, skaalautuvuus, korkean käytettävyys, suorituskyvyn valvonta sekä multi-domain tuki. (ECI 2017.)

KUVIO 7 IP/MPLS ja MPLS-TP:n suhde

MPLS-TP korvaa MPLS-ohjaustason ominaisuuksia, jotka vastaavat layer 3 -reititystietojen ja leimainformaation levityksestä. MPLS-TP voi kuljettaa layer 3, 2 ja 1 -palveluita, eikä vaadi mitään tiettyä fyysisen kerroksen siirtotapaa toimiakseen. LSP:t ja pseudowiret provisioidaan staattisesti käyttäen verkonhallintajärjestelmää (NMS, Network Management System). Tämä on vastaava tapa kuin vanhoissa TDM-siirtojärjestelmissä, esimerkiksi SDH:ssa. Kuvissa 8 ja 9 näkyvät IP/MPLS:n ja MPLS-TP:n hallinta- ja ohjaustasojen erot. (ECI 2017.)



KUVIO 8 MPLS-TP hallinta- ja ohjaustaso



KUVIO 9 IP/MPLS hallinta- ja ohjaustaso

MPLS-TP on laajalti hyväksytty seuraaja perinteisille TDM-siirtotekniikoille, kuten PDH ja SDH. MPLS-TP on tarkoitettu erityisesti kriittisille verkoille käytettäväksi. Yksi MPLS-TP:n merkittävimmistä eduista on se, että MPLS-TP käyttää kaksisuuntaisia polkuja. Tämä yksinkertaistaa hallittavuutta ja parantaa suorituskykyä. (ECI 2017.)

4 SUOJAUKSEN VIESTIYHTEYDET

Suojauksen viestiyhteydet ovat tärkeä osa Suomen kantaverkon toimintaa, sillä suojauslaitteet vaativat vakaan symmetrisen yhteyden jatkuvaan viestintään releiden välille. Viestiyhteyksien tulee sietää ulkoisia häiriöitä ja tarjota erittäin suurta luotettavuutta. 400 kV suojauksen viestiyhteydet on kahdennettu, sillä niiden toimimattomuus on koko järjestelmän käyttövarmuuden kannalta suuri uhka. 220 kV suojauksen viestiyhteyksiä ei ole kahdennettu ja 110 kV:n johdoilla suojauksen viestiyhteys on vain tarvittaessa. (Kantaverkkowiki 2017.)

Suojausaika koostuu kolmesta eri osasta; signalointiaika, releiden laukaisuaika ja katkaisijoiden laukaisuaika. Näiden kolmen tekijän yhteenlaskettu aika 400 kV -johdolla tulisi olla alle 100 ms, joka on 50 Hz:n taajuudella viisi sykliä. Useimmat suurjännitejärjestelmät kestävät viiden syklin pituisia vikoja aiheuttamatta vahinkoa johtimille tai järjestelmän muille osille, kuten laitteille. (RAD Data Communications 2011.)

4.1 Suojauksen viestiyhteyksiin liittyvät standardit

Suojauksen viestiyhteyksien fyysiset ja sähköiset ominaisuudet sekä nopeudet määritetään erilaisilla standardeilla. Standardien käytöllä varmistetaan tiettyjen asioiden yhteensopivuus esimerkiksi eri laitevalmistajien kesken.

4.1.1 ITU-T G.703

ITU-T:n G.703 on standardi, josta on tullut perusta piirikytkentäisille tietoliikenneverkoille. G.703 määrittää suositellut fyysiset ja sähköiset ominaisuudet hierarkisille bittinopeuksille, jotka on määritetty standardeissa G.702 (PDH) ja G.707 (SDH). Näiden määrityksien avulla dataa voi siirtää joko kierretyssä 120 ohmin (Ω) parikaapelissa tai kahdessa 75 ohmin koaksiaalikaapelissa.120 ohmin johdoissa käytetään RJ-45 -liittimiä ja 75 ohmin johdoissa käytetään BNC-liittimiä. G.703 on laajalti käytetty liitäntä suojauslaitteissa. (ITU-T 2016.)

4.1.2 64 kbit/s optisen liitynnän standardi IEEE C37.94

IEEE C37.94 on standardi ohjelmoitavalle maksimissaan 12 kertaa 64 kbps optiselle liitynnälle ala-aseman sisäisten telesuojaus- ja multiplekserilaitteistojen välille. Fingridillä on kuitenkin käytössä vain yksi aikaväli.

IEEE C37.94 määrittää siirtotiellä käytettäväksi monimuotokuitua. C37.94 asettaa vaatimukset sekä fyysiselle yhteydelle että viestinnän ajoitukselle. C37.94 määrittää kellon palautumisen, viiveiden toleranssit, fyysisen kytkentätavan ja laitteistojen vikatoiminnot kaikille linkkien vioille. (SEL 2012.)

4.2 Vaatimukset laitteistolle ja yhteydelle

Suojauksen viestiyhteyksien käyttö asettaa vaatimuksia käytetyille laitteille ja toiminnoille. Myös itse yhteydelle Fingridissä asetettu seuraavat vaatimukset.

Yksittäisen suojauksen viestiyhteyden käytettävyyden tulee olla ≥ 99,9 % eli yhteys saa olla poikki alle yhdeksän tuntia vuodessa, kun taas kahdennetulla yhteydellä vastaavat arvot ovat ≥ 99,97 % ja ≤ 2,6 tuntia. (1) Kahdennettujen yhteyksien tapauksessa tulee olla kahdennettu kanavointilaitteet/releiden liitäntälaitteet, tietoliikennelaitteet, fyysiset reitit sähköasemalla ja sieltä ulos vasta-asemalle. Pulssin pituuden eron sekä differentiaali että distanssireleen tapauksessa tulee olla korkeintaan 10 %. (Requirements for telecommunication for protection purposes 2008.)

Kaikkien suojaukseen liittyvien laitteiden tulee sietää korkeita EMC-olosuhteita ilman, että niiden toiminta häiriintyy. Lisäksi laitteiden tulee käyttää standardisoituja liitäntöjä. (Requirements for telecommunication for protection purposes 2008.)

Distanssireleen käyttäminen suojauksen viestiyhteyksissä edellyttää käytettävältä yhteydeltä, tyypistä riippumatta alle 25 ms siirtoaikaa

suuntaansa. Siirtoaikojen ero eri suuntiin tulee olla alle 10 ms. (Requirements for telecommunication for protection purposes 2008.)

Differentiaalirele vaatii distanssirelettä nopeamman siirtoajan. Siirtoajan tulee olla alle 15 ms suuntaansa. Siirtoaikojen eron, huojunnan ja vaihtelun tulee olla alle 0,9 ms. Askelmuutoksen, esimerkiksi uudelleenreitityksen tapauksessa tulee olla alle 3 ms. Askelmuutoksen tulee olla samanaikainen ja symmetrinen kumpaankiin suuntaan. Vaikka SDH-verkossa on mahdollista käyttää uudelleenreititystä, Fingridin tapauksessa sitä ei saa käyttää ilman erillistä lupaa, suunnitelmaa ja stabiiliusmittauksia. (Requirements for telecommunication for protection purposes 2008.)

4.3 Siirtotiet

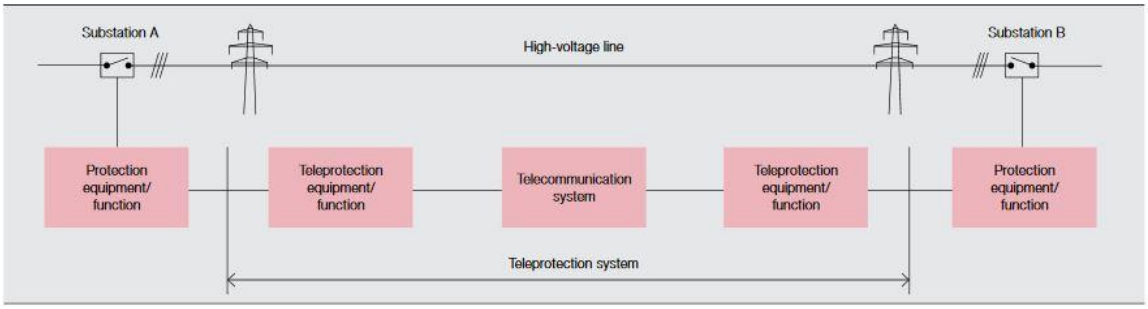
Optinen kuitu on suositeltu siirtotie suojauksen viestiyhteyksille, sillä kuitu on lähes immuuni sähkömagneettisille häiriöille ja sillä on suuri tiedonsiirtokapasiteetti. Optista kuitua voidaan käyttää sähköasemien sisäiseen viestintään ja sähköasemien väliseen viestintään pitkilläkin matkoilla. (Kantaverkkowiki 2017.)

Kuparikaapeli ei sovellu pitkälle matkalle käytettäväksi, sillä signaali heikkenee ja vääristyy helposti. Kuparikaapeli ei myöskään ole immuuni sähkömagneettisille häiriöille kuten optinen kuitu. Uusia kupariyhteyksiä ei enää rakenneta. (Kantaverkkowiki 2017.)

Hyvin suunniteltuna ja toteutettuna digitaalisia radiolinkkejä voidaan käyttää suojauksen viestiyhteyksiin. Digitaalisten radiolinkkien taajuudet ovat 6 - 18 GHz:n välillä. Tietyillä taajuuksilla toimivat radiolinkit ovat alttiita luonnonilmiöille, kuten ukkoselle ja vesisateelle, jotka aiheuttavat virheitä ja katkoksia yhteyteen. Nämä ovat sähköverkon kannalta juuri niitä tilanteita, joissa suojauksen pitäisi toimia. Radiolinkkien hyvä puoli on niiden kantavuus, joka on jopa 50 km. Tämä siis tarkoittaa, ettei kaapelia tarvitse rakentaa 50 km:n matkalle ollenkaan, ja radiolinkki on usein myös siksi edullinen ratkaisu. (Kantaverkkowiki 2017.)

4.4 Käytetyt aikajakoiset tiedonsiirtojärjestelmät

Nykyisin sähköverkon suojauksen viestiyhteyden vaihtoehdot ovat olleet TDM-pohjaiset ratkaisut PDH ja SDH. PDH- ja SDH-siirtoverkoissa signaalin kulkuaikaviiveen vaihtelu on vähäistä, ja siksi ne soveltuvat hyvin suojauskäyttöön. Kuviossa 10 on esitetty tyypillinen suojausjärjestely kantaverkossa.



KUVIO 10 Tyypillinen suojausjärjestely

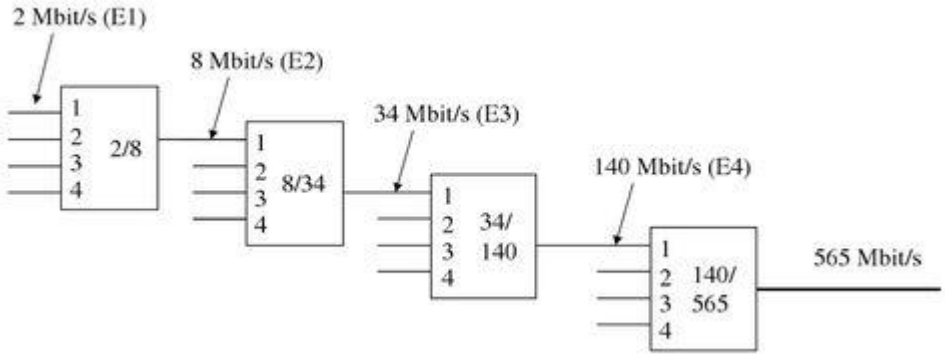
4.4.1 Plesionkroninen digitaalinen hierarkia (PDH)

Perinteiset digitaaliset siirtojärjestelmät jaetaan plesiokronisiin (PDH) ja synkronisiin (SDH) -järjestelmiin. PDH on kanavointitekniikka, jossa on mahdollista pakata alemman tason 4 yhteyttä yhteen, hieman nelinkertaista isompaan yhteyteen. PDH eli plesiokronisessa järjestelmässä verkon eri osat eivät ole täysin synkronisia, toisin kuin SDH-verkossa. SDH on synkroninen järjestelmä ja tarvitsee siksi äärimmäisen tarkan kellon. Kellona voidaan käyttää esimerkiksi GPS- tai atomikelloa. PDH-verkossa laitteet voidaan synkronoida jokainen oman

kellonsa mukaan ja tästä syystä PDH on plesionkroinen järjestelmä. (IJSRET 2014.)

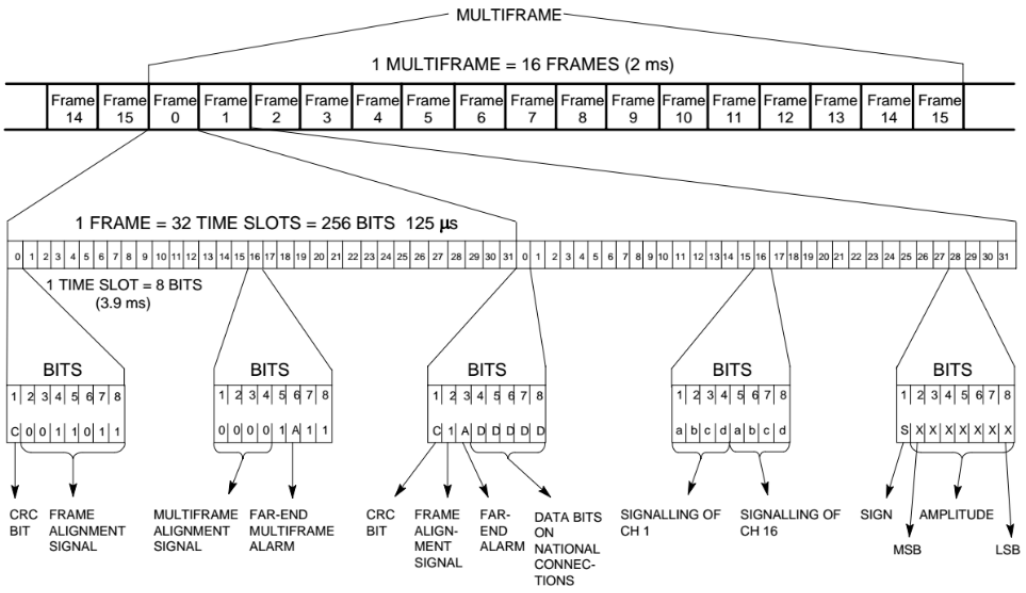
PDH on alun perin tarkoitettu käytettäväksi puhelinverkoissa ja se on SDH:n tapaan aikajakoinen järjestelmä (TDM, Time-Division Multiplexing), joka tarkoittaa sitä, että eri yhteyksiä voidaan lähettää samalla signaalilla jakamalla signaali pieniin segmentteihin, eli aikaväleihin. (IJSRET 2014.)

PDH:n kansainvälisesti sovitut nimellisnopeudet ovat Euroopassa 2 (E1), 8 (E2), 24 (E3), ja 140 (E4) Mbit/s. Näiden lisäksi on myös nopeudella 565 (E4) Mbit/s toimivia järjestelmiä, mutta tätä nopeutta ei ole standardisoitu. (IJSRET 2014.)



KUVIO 11 PDH periaatekuva (Nokia Plesiochronus Digital Hierarchy)

Kuviossa 12 näkyy PDH-järjestelmän toimintaperiaate. PDH-järjestelmä toimii porrastetusti, eli jos halutaan yhdistää E1- ja E4-järjestelmät, tarvitaan myös E2- ja E3-tasojen laitteet. Suuri laitemäärä on yksi PDH:n huonoista puolista. Kuviossa 11 on esitetty ITU-T:n standardin G.704 mukaisen 2 Mbit/s signaalin kehysrakenne. Kehyksen pituus on 125 μs ja koostuu 32 aikavälistä, jotka on numeroitu 0-31. Jokainen aikaväli sisältää kahdeksan bittiä ja on pituudeltaan 3,9 μs. Koska kehys koostuu 256 bitistä ja toistuu 8000 kertaa sekunnissa, tulee nopeudeksi 2048 kbit/s. (Nokia 2006.)



KUVIO 12 2 Mbit/s signaalin kehysrakenne (Nokia 2 Mbit/s frame structure 2006)

4.4.2 Synkroninen digitaalinen hierarkia (SDH)

SDH perustuu 1980-luvun lopussa USA:ssa kehitettyyn SONET-standardiin. SONET määrittelee tiedonsiirtotavan ja nopeudet. ITU-T vastaa SDH:n kansainvälisestä standartoinnista. SDH perustuu pääasiassa optisten valokuitujen käyttöön. (Fiberoptic 2017.)

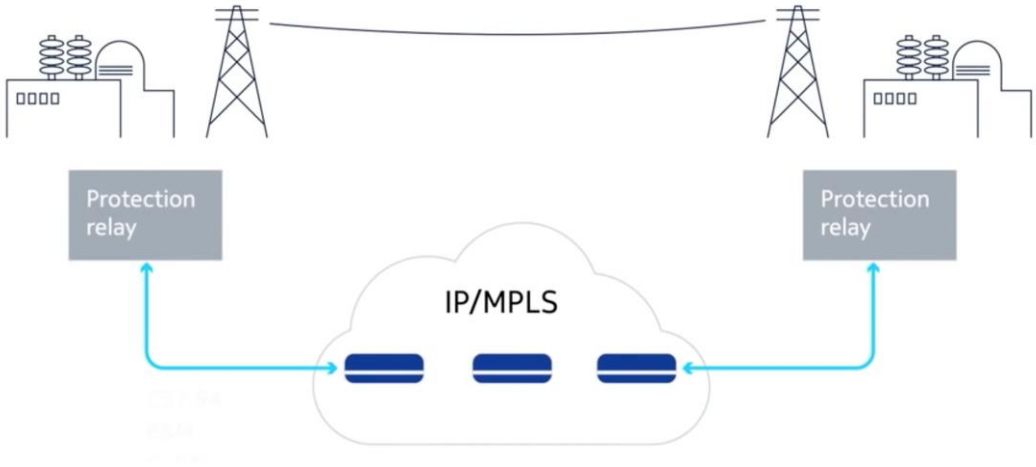
SDH kehitettiin, kun huomattiin, ettei PDH enää täytä operaattoreiden tarpeita. Yksi SDH-järjestelmän suurimpia etuja PDH:n nähden on se, ettei kaikkia siirtonopeustasoja tarvitse purkaa siirrettäessä esimerkiksi 2 Mbit/s signaalia 155 Mbit/s järjestelmässä. SDH:n etuja PDH:hon nähden ovat esimerkiksi pienentynyt laitemäärä vastaavien nopeuksien saavuttamiseksi, pienentyneen laitemäärän johdosta myös lisääntynyt käyttövarmuus, käyttökustannukset ja isoimpana etuna järjestelmän hallintaominaisuudet osana isompaa siirtoverkkoa. Taulukossa 1 on esitetty SDH-järjestelmän siirtonopeudet. (Fiberoptic 2017.)

TAULUKKO 1 SDH-järjestelmän siirtonopeudet

STM-taso	Siirtonopeus (Mbit/s)
STM-1	155,52
STM-4	622,08
STM-16	2488,32
STM-64	9953,28

5 MPLS-VERKKO SUOJAUSKÄYTÖSSÄ

Kuviossa 13 on esimerkkitapaus MPLS-verkon hyödyntämisestä suojauskäyttöön. Kuviossa perinteinen PDH/SDH-verkko on korvattu IP/MPLS-tekniikalla käyttäen näennäisjohdinta, pseudowire.



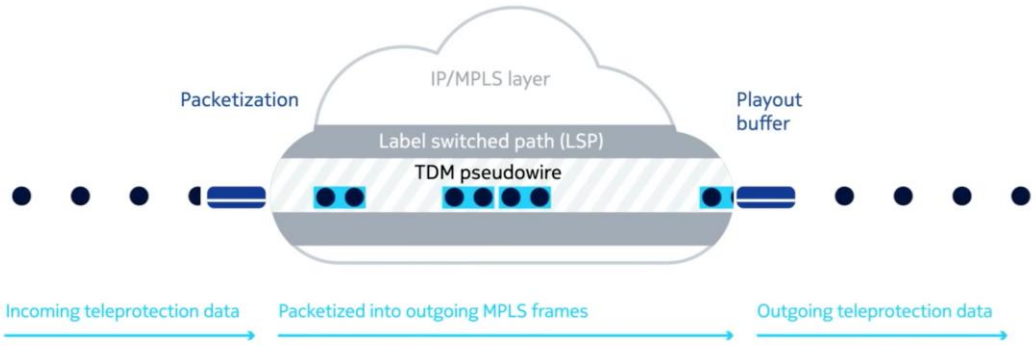
KUVIO 13 MPLS-verkon hyödyntäminen suojauskäytössä

Pakettikytkentäisissä verkoissa ei käytetä SDH:n tapaan synkronointia. Tämä on olennainen asia suojauskäytössä, sillä nämä kriittiset verkot luottavat tarkkaan ajoitukseen ja synkronointiin välittäessään mittaustietoja suojareleiden välillä. (ECI 2017.)

Pakettikytkentäisen verkon synkronointitekniikoita ovat SyncE (Synchronous Ethernet) ja 1588v2. Näistä yleisempi on 1588v2 SyncE:n tuen puutteen vuoksi. Näitä kahta voidaan myös käyttää yhdessä synkronointiin ja ajan siirtoon paremman tarkkuuden saavuttamiseksi.

1588v2:lla voidaan saavuttaa jopa alle mikrosekunnin tarkkuus lähiverkossa. 1588v2 on ToP (Timing over Packet) -tekniikka, joka perustuu edestakaiseen aikaleimojen vaihtoon. Koska 1588v2 on pakettipohjainen tekniikka, ajoitustietoja kuljettavat paketit kilpailevat verkon muuta dataa kuljettavien pakettien kanssa verkon resursseista. Tämä vaikuttaa verkon synkronoinnin suorituskykyyn ja sitä kutsutaan PDV:ksi (Packet Delay Variation), joka tarkoittaa yksinkertaisesti paketin viiveen vaihtelua. Jotta tältä ongelmalta vältyttäisiin, tarjoaa esimerkiksi MPLS-TP QoS:n lisäksi siihen vaadittavan ominaisuuden, kaksisuuntaiset reitit, joiden avulla voidaan taata riittävä suorituskyky verkon tarkalle synkronoinnille. IP/MPLS-verkossa Nokian kehittämä ADC (Asymmetrical Delay Control) on tarkoitettu poistamaan satunnaiset pakettien viiveiden vaihtelut ja palauttamaan viiveiden symmetrian ja täten estämään suojauslaitteiden virhelaukaisut. (ECI 2017; Nokia 2016.)

Pakettikytkentäinen verkko ei välitä luonnostaan PDH/SDH-verkkosignaaleja. Tämän takia piirikytkentäisiä suojausviestejä siirrettäessä MPLS-verkon läpi täytyy siirtoverkon alkupäässä muuttaa suojaussignaalit pakettiverkkoon sopivaksi, eli jakaa paketteihin, ja loppupäässä purkaa takaisin TDM-signaaliksi. Pakettikytkentäisessä verkossa dataa lähetetään siirtotielle synkronoimattomasti ja siksi piirikytkentäisiä signaaleja siirtäessä tarvitaan puskuri, joka vastaanottaa paketit ja välittää eteenpäin synkronoidusti. Kuviossa 14 havainnollistava kuvio puskurin toiminnasta yhdessä MPLS-pseudowiren kanssa. Kuviosta huomataan, että signaalit ennen ja jälkeen IP/MPLS-verkon kulkevat tietyin aikavälein ja verkon sisällä taas erikokoisissa paketeissa vaihtelevin väliajoin. Puskurilla kompensoidaan siirtoverkon aiheuttamaa pakettien viiveiden vaihtelua. (Nokia 2016.)



KUVIO 14 Puskurin toimintaperiaate

Nykyään markkinoilla on jo suojauslaitteita, joissa on ethernet-liityntä. Ethernet-liityntä mahdollistaa suojausviestien lähettämisen ja vastaanottamisen ilman muunnosta TDM-signaalista pakettiverkkoon sopiviksi paketeiksi. Alcatel-Lucentin erityisolosuhteissa tehdyn testin mukaan käyttämällä Siemensin 7SD52 -suojarelettä ja E1-liityntää, viivearvoksi on saatu 1,15 ms. Vastaavasti käyttämällä Ethernet-liityntää on viiveeksi saatu jopa 100 µs. Tämän mahdollistaa se, että signaalia ei tarvitse muuttaa erikseen pakettiverkkoon sopivaksi. Testi ei vastaa oikeaa käyttötilannetta, mutta paljastaa eri liityntöjen tuoman eron ja signaalin muuttamisesta johtuvan viiveen. (Energati 2015.)

5.1 MPLS-verkon testaaminen ja liikenteen luokittelu

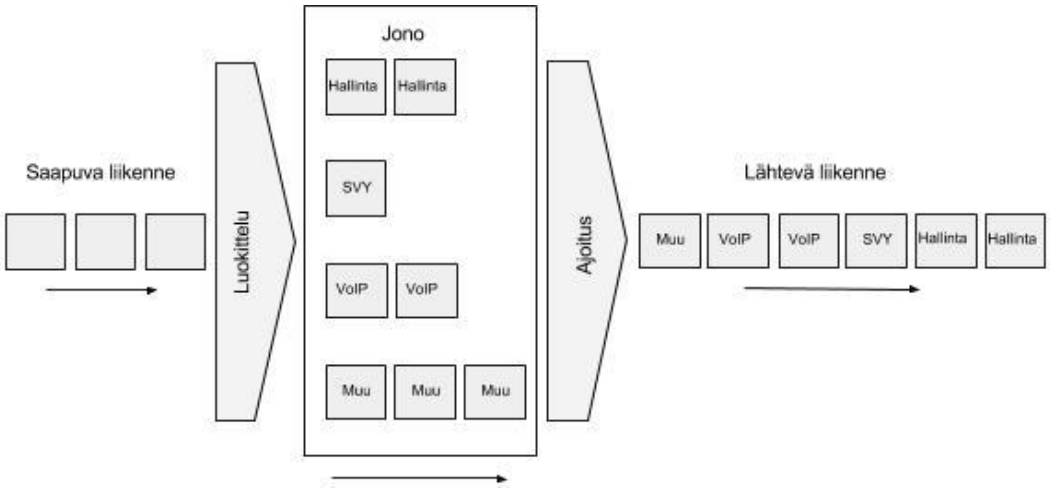
Jotta MPLS-verkon soveltuvuudesta suojaskäyttöön olisi varmuus, tulisi sitä testata monin erilaisin testein simuloidulla sähkönsiirtoverkolla. Suurin osa testeistä liittyy verkon suorituskykyyn, mutta myös tietoturva on tärkeä asia kriittisen verkon tapauksessa. MPLS-verkossa suurin huolenaihe on viive ja viiveen vaihtelu. MPLS-verkkoa tulisi testata ainakin seuraavilta osin:

- siirtoaika

- luotettavuus
- palautumisaika
- viiveen vaihtelu
- vikasietoisuus
- ajoitus.

Testit tulisi suorittaa sekä ilman taustaliikennettä että taustaliikenteen kanssa, jotta verkon suorituskyky voitaisiin varmistaa myös ruuhkaisessa tilanteessa. MPLS-verkkoa tulisi testata käyttämällä QoS-palvelulla korkeaksi priorisoitua liikennettä ja lisäksi niin sanotulla ”Best Effort” -menetelmällä, joka tarkoittaa alinta mahdollista prioriteettiä, eli jos kaistaa ei ole, niin dataa ei siirretä. Muun liikenteen ei tulisi vaikuttaa korkean prioriteetin eli suojausviestien kulkuaikoihin käytettäessä liikenteen priorisointia.

Liikenteen luokittelu on yksi testaamisen tärkeimmistä osa-alueista. Jotta priorisointi olisi mahdollista, tulisi kaikki verkon läpi kulkeva liikenne luokitella, jotta kriittinen liikenne saa varmasti tarvitsemansa kaistan. MPLS-leiman kolmea Traffic Class -bittiä voidaan käyttää yhteensä kahdeksan eri prioriteettiluokan määrittämiseen. Liikennettä voisi luokitella esimerkiksi seuraavasti: suojaussignaalit, verkon hallinta ja valvonta, ääni- ja videopalvelut ja viimeiseksi yleinen verkon käyttö, esimerkiksi Internetin selaaminen. Liikenneluokat määritetään palvelun tai toiminteen kriittisyyden mukaan. Suojaussignaalit sekä verkon hallinta ja valvonta ovat verkon kriittisimmät palvelut ja siksi niiden tulisi olla kaksi korkeinta prioriteettiluokkaa. Näiden jälkeen seuraavaksi viivekriittisimmät palvelut ovat ääni- ja videopuhelut, joiden paketit tulee siirtää tietyssä ajassa, tai ne vanhenevat. Muut, kuten etähallintayhteydet tulisi määrittää toisiksi alimman prioriteettitason liikenteeksi. Vähiten tärkeät, kuten ala-asemien WLAN-yhteydet tulisi määritellä alimmalle mahdollisimmalle prioriteetille. Kuviossa 15 havainnollistetaan QoS:n toimintaa esimerkkitapauksessa. Tässä kuviossa liikenne luokitellaan neljään eri ryhmään, jotka ovat verkon hallinta, suojauksen viestiyhteydet, VoIP ja muu liikenne.



KUVIO 15 QoS:n toimintaperiaate

Tietoturvan testaaminen suorituskykymittauksissa ei ole olennaista. Salaus ei juurikaan vaikuta suorituskykymittauksiin, joissa mitataan pääasiassa viivettä, ei kaistanleveyttä. Yhteys tulisi kuitenkin salata päästä päähän, jotta dataa ei pystytä muuttamaan siirtotiellä. Salaus ja purku voidaan toteuttaa esimerkiksi NGE (Network Group Encryption) -menetelmällä, jolla voidaan salata IEEE C37.94:n määrittelemää liikennettä MPLS-verkossa AES256-salausalgoritmilla. (University of Strathclyde 2016.)

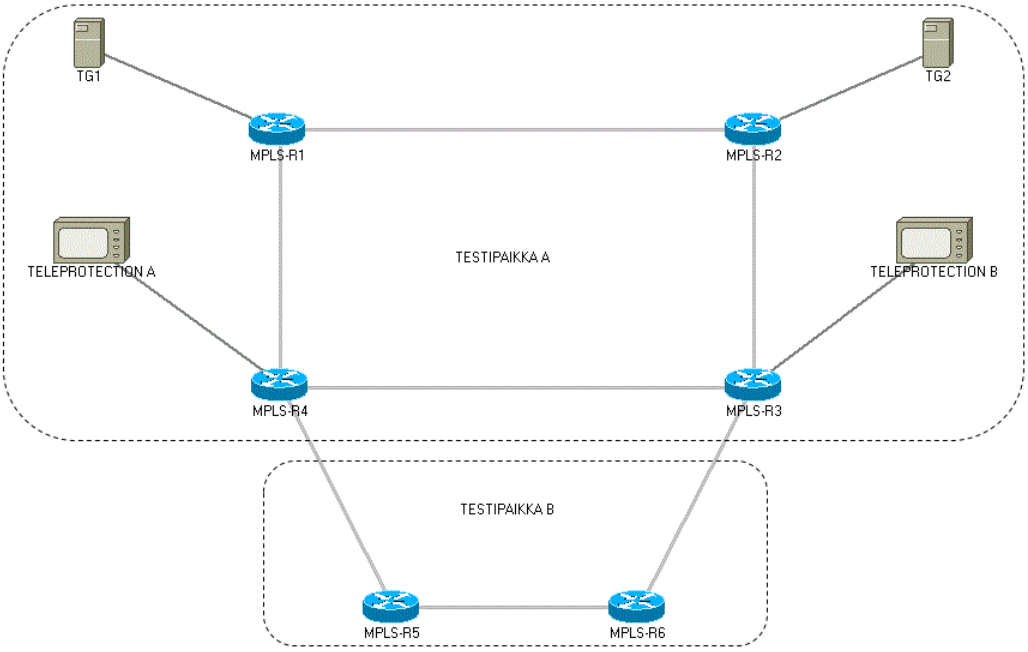
5.2 Testijärjestely

Testilaitteiden tulisi olla oikeassa suojaustilanteessa käytettäviä laitteita, tai vähintään vastaavia ominaisuuksiltaan. Tämä tarkoittaa siis sitä, että myös laitteiden liitäntöjen tulee olla täysin yhteensopivia muiden käytettävien laitteiden kanssa.

Kuviossa 16 on esitetty mahdollinen testijärjestely kahden eri paikan välillä, testipaikat A ja B. Kuviossa näkyy kahden eri suojauslaitteen välinen yhteys toteutettuna MPLS-verkossa. Kuten oikeassakin tilanteessa, esimerkiksi testipaikassa B sijaitsee valvomo, josta verkkoa

hallitaan. Testijärjestely mahdollistaa erilaisten reittien testaamisen reitittämällä liikennettä eri tavoin.

Kuviossa 16 esitetyssä testijärjestelyssä on kuusi MPLS-reititintä, MPLS-R1-R6, kaksi verkon suojauslaitetta TELEPROTECTION A ja B sekä kaksi liikennegeneraattoria TG1 ja TG2. Liikennegeneraattoreilla tuotetaan niin sanottua taustaliikennettä häiriöksi, jotta priorisointia voidaan testata. Liikennegeneraattoreiden tulisi pystyä tuottamaan tarpeeksi liikennettä täyttääkseen kokonaan käytetyn linkin verkossa. Suojauslaitteiden tulisi olla oikeita, ei suojausviestejä simuloivia laitteita, jotta testeistä tulisi mahdollisimman todenmukaisia. Testin suorittamiseksi tarvitaan lisäksi verkon ajoituksen synkronointiin, viiveiden ja BER:n mittaamiseen soveltuvat laitteet, joita kuviossa 16 ei esitetä.



KUVIO 16 MPLS-verkon testijärjestely

Kuvion 16 mukaisessa testijärjestelyssä voidaan testata viivettä, luotettavuutta, palautumisaikaa, viiveen vaihtelua ja vikasietoisuutta käyttäen G.703/64k, G703/E1 ja C37.94 palveluita. Testissä on mahdollista reitittää liikennettä monin eri tavoin. Tärkeimmät testit ovat viive ja viiveen vaihtelu. Viivettä ja viiveen vaihtelua voidaan testata mittaamalla yhdensuuntaisen siirron kulkuaikaa ja vertaamalla tuloksia toisiinsa. Tyypillisesti viiveen minimoimiseksi ensisijainen reitti on lyhin ja vähiten hyppyjä omaava reitti. Tässä tapauksessa se tarkoittaisi reittiä MPLS-R4 - MPLS-R3. Jotta testi olisi totuudenmukainen, tarvitaan liikennegeneraattorien TG1 ja TG2 tuottamaa taustaliikennettä täyttämään suojausyhteyden käyttämä siirtotie. Oikein priorisoituna taustaliikenteen ei tulisi vaikuttaa suojausviestien viiveisiin, sillä korkeamman prioriteetin liikenteelle pitäisi olla aina taattu kaista. Testin tulosta voidaan verrata ilman taustaliikennettä suoritettuihin testeihin priorisoinnin toimivuuden toteamiseksi.

Luotettavuuden testaamisella tarkoitetaan pakettien hukkumista siirtotiellä (packet loss) ja virheellisten pakettien suhdetta virheettömiin paketteihin (bit error rate). Myös verkon ajoituksen tarkkuus on osa verkon luotettavuutta ja sitä tulisi mitata siihen soveltuvalla tarkalla mittalaitteella. Verkon luotettavuus on tärkeä osa suojauksen toimintaa, sillä matkalla hukkuneiden pakettien vuoksi voi suojauslaitteilta jäädä jokin vika huomaamatta ja näin aiheuttaa vahinkoa järjestelmälle.

Verkon palautumisaikaa voidaan testata esimerkiksi irrottamalla kaapeli tai sammuttamalla laitteita ja käynnistämällä uudelleen. Samoilla menetelmillä on mahdollista testata myös vikasietoisuutta. Vikasietoisuutta parantaisi automaattinen uudelleenreititys, jota ei Fingridin tapauksessa kuitenkaan käytetä. Manuaalista uudelleenreititystä toissijaista reittiä pitkin voidaan käyttää, jotta saadaan vertailukohteita.

Testit tulisi suorittaa käyttäen eri priorisointiluokkia erilaisten tulosten saavuttamiseksi. Samat testit tulisi suorittaa myös käyttäen vanhempaa, SDH-tekniikkaa, joihin MPLS-verkolla saatuja tuloksia voisi verrata.

6 YHTEENVETO JA JOHTOPÄÄTÖKSET

Hyväksi ja luotettavaksi todetusta tekniikasta uuteen siirtymisessä on iso kynnys, varsinkin jos kyseessä on jokin kriittinen palvelu, kuten kantaverkon suojausyhteydet. Tämän kynnyksen ylittäminen vaatii tutkimus- ja selvitystyötä uudesta teknologiasta. MPLS-tekniikkaan siirtymistä ei tulisi pelätä, sillä siitä on kehitetty äärimmäisen hyvin toimiva ja luotettava ratkaisu moniin eri tarkoituksiin. MPLS-tekniikka tarjoaa luotettavan, joustavan ja hallittavuudeltaan sekä ylläpidettävyydeltään hyvän verkkoratkaisun myös suojauksen viestiyhteyksille.

Suojauksen viestiyhteyksien tapauksessa on jo kauan luotettu TDM-teknologiaan, jossa viiveet ja viiveen vaihtelut ovat todella pieniä. MPLS-verkko on ollut jo kauan käytössä, mutta sitä ei ole hyödynnetty laajasti kantaverkon suojauksessa. MPLS-verkko tarjoaa palveluita vanhojen PDH/SDH-verkkojen korvaamiseksi ja luotettavan pieniviiveisen siirtotavan suojauksen viestiyhteyksille. Koska MPLS-verkko käyttää ennalta määrättyjä reittejä, se takaa verkon alusta loppuun saakka toimivan liikenteen priorisoinnin, QoS:n. MPLS-TP on erityisesti TDM-pohjaisten siirtotapojen korvaajaksi tarkoitettu yksinkertaistettu MPLS-verkko.

MPLS-verkko tukee SDH:n tavoin nopeaa, jopa alle 50 millisekunnin automaattista uudelleenreititystä, mutta tässä tapauksessa sitä ei tulisi erinäisistä syistä johtuen käyttää. Automaattinen uudelleenreititys voi siirtää esimerkiksi vastapään suojausliikenteen vaihtoehtoiselle reitille, josta voi seurata viiveen nousua ja epäsymmetrisyyttä, ja tästä johtuen turhia laukaisuja. Toinen syy on reitin vaihtaminen varareitille kenenkään huomaamatta. Tällöin käytössä olevan reitin hajotessa ei varareittiä olisikaan, ja suojausyhteys olisi kokonaan poikki. Automaattista uudelleenreititystä voisi käyttää vain olosuhteissa, joissa ensisijaisen ja toissijaisen reitin viiveiden ero ja vaihtelu olisi minimaalisia ja yhteyden kaikki muutokset huomattaisiin reaaliajassa, eikä pääsisi syntymään edellämainittuja tilanteita.

MPLS-verkko soveltuu suojauksen viestiyhteyksiin monien eri palvelujensa ansiosta, mutta tämä täytyisi varmistaa suorittamalla erilaisia testejä käyttäen MPLS-tekniikkaa. MPLS-tekniikkaa ja ethernet-liityntäisiä suojauslaitteita käyttämällä kokonaisviivettä voitaisi mahdollisesti jopa pienentää nykyisestä. MPLS-verkot tullee yleistymään juurikin sähköverkon suojauskäytössä tulevina vuosina.

MPLS on hyväksi havaittu ja laajalti käytetty verkkoratkaisu Toisin kuin SDH, MPLS ei ole vielä vuosiin katoamassa mihinkään, eikä menettämässä rooliaan eniten käytettynä ulkoverkkoratkaisuna. MPLS on kuitenkin kalliimpi vaihtoehto esimerkiksi Internet-ratkaisuille yhdistettäessä lähiverkkoja toisiinsa.

Palveluiden testaaminen tuotannossa on tulevaisuudessa vähenemään päin. Kun kyseessä on jokin kriittinen palvelu tai verkko, tulee se testata hyvin ennen käyttöönottoa. Tulevaisuuden verkkopalveluiden käyttäjämäärät kasvavat jatkuvasti ja palveluiden vikaantuminen voi aiheuttaa suurta tappiota palveluntarjoajalle niin maineen kuin talouden kannalta. Testaamiseen tulisikin panostaa aiempaa selvästi enemmän. Tulevaisuudessa palveluiden ja verkkojen testaamisen tärkeys korostuu aina kasvavassa digitaalisessa maailmassa.

LÄHTEET

Alvarez, S. 2006. QoS for IP/MPLS Networks. USA:Cisco Press.

Balchunas, A. 2010. QoS Classification and Marking [viitattu 26.4.2017]. Saatavissa: http://www.routeralley.com/guides/qos_classification.pdf

Cisco 1999. Quality of Service Networking [viitattu 30.1.2017]. Saatavissa: http://docwiki.cisco.com/wiki/Quality_of_Service_Networking

Cisco 2005. Layer 2 VPN Architectures: Understanding Any Transport over MPLS [viitattu 20.1.2017]. Saatavissa: http://www.ciscopress.com/articles/article.asp?p=386788&seqNum=2

Cisco 2016. MPLS FAQ For Beginners [viitattu 26.2.2017]. Saatavissa: http://www.cisco.com/c/en/us/support/docs/multiprotocol-label-switching-mpls/mpls/4649-mpls-faq-4649.html#anc4

ECI 2017. MPLS-TP FOR MISSION-CRITICAL NETWORKS [viitattu 25.2.2017]. Saatavissa: https://www.ecitele.com/media/1638/mpls-tp-for-mission-critical-networks-wp-f.pdf

Energati 2015. Transitioning Teleprotection And SCADA To IP/MPLS [viitattu 12.1.2017]. Saatavissa: https://www.engerati.com/article/transitioning-teleprotection-and-scada-ipmpls

Fingrid Oyj 2008. Requirements for telecommunication for protection purposes [viitattu 16.2.2017]. Word-dokumentti.

Fingrid Oyj 2013. Line Protection - Johtosuojaus [viitattu 16.2.2017]. Word-Dokumentti.

Fingrid Oyj 2014. Suojauksen viestiyhteydet -koulutus [viitattu 8.2.2017]. Koulutusmateriaali.

Fingrid Oyj 2016. Kantaverkkowiki [viitattu 8.2.2017]. Saatavissa: Fingrid Oyj Intranetissa:

http://wiki.fingrid.fi/pages/viewpage.action?title=Kantaverkkowiki&spaceKey=kanta

IEEE 2013. Packet routing and information distribution in Multiprotocol Label Switching [viitattu 18.2.2017]. Saatavissa IEEE Xplore -tietokannassa: http://ieeexplore.ieee.org/document/6563355/.

IETF 2006. Encapsulation Methods for Transport of Ethernet over MPLS Networks [viitattu 27.3.2017]. Saatavissa: https://tools.ietf.org/html/rfc4448

IETF 2011. MPLS Transport Profile (MPLS-TP) Survivability Framework [viitattu 14.2.2017]. Saatavissa: https://tools.ietf.org/html/rfc6372

ITU-T 2016. G.703 : Physical/electrical characteristics of hierarchical digital interfaces [viitattu 20.2.2017]. Saatavissa: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-G.703-201604-I!!PDF-E&type=items

Juniper 2016. Understanding MPLS Label Operations on EX Series Switches [viitattu 23.2.2016]. Saatavissa: https://www.juniper.net/documentation/en_US/junos/topics/concept/mpls-label-operations-ex-series.html

Metaswitch Networks 2001. Protection And Restoration In MPLS Networks [viitattu 22.2.2017]. Saatavissa: http://www.olddog.co.uk/mplsprotwp2.pdf.

Nanog 2016. MPLS for Dummies [viitattu 22.2.2017]. Saatavissa: https://www.nanog.org/meetings/nanog49/presentations/Sunday/mpls-nanog49.pdf

Networklessons 2017. MPLS Layer 3 VPN Explained [viitattu 1.2.2017]. Saatavissa: https://networklessons.com/mpls/mpls-layer-3-vpn-explained/

Nokia 2006. TPS 64 TELEPROTECTION SIGNALLING EQUIPMENT [viitattu 22.2.2017]. Ohjekirja.

Nokia 2016. Mission-critical communications networks for power utilities [viitattu 19.1.2017]. Saatavissa: https://resources.alcatel-lucent.com/?cid=180690

RAD Data Communications 2011. Network Migration for Utilities, Teleprotection over Packet [viitattu 1.2.2017]. Saatavissa: http://rycom.net/userfiles/file/Teleprotection-over-Packet-Solution-Paper.pdf

SEL 2012. Improve safety and protect equipment by upgrading to fiber-optic teleprotection links [viitattu 10.1.2017]. Saatavissa: https://cdn.selinc.com/assets/Literature/Product%20Literature/Flyers/C37-94_PF00147.pdf?v=20151016-140933

Springer Publishing 2014. Communication Networks for Smart Grids: Making Smart Grid Real [viitattu 10.2.2017]. Saatavissa: https://www.google.fi/url?sa=t&rct=j&q=&esrc=s&source=web&cd=7&cad=rja&uact=8&ved=0ahUKEwizlvWA5zSAhVJjCwKHUiKBJcQFghKMAY&url=https%3A%2F%2Flib.lhu.edu.vn%2FViewFile%2F11983%2FCommunication%2520Networks%2520for%2520Smart%2520Grids%2C%2520Kenneth%2520C%2520Budka%2C%2520Springer%25202014.pdf&usg=AFQjCNEEKrYne7OyJ4yzotkrX5nCbvHmQQ&sig2=8XXNyYCV2fwqZTdZzzqacQ&bvm=bv.150475504,d.bGg

University of Strathclyde 2016. Validating Secure and Reliable IP/MPLS Communications for Current Differential Protection [viitattu 5.3.2017]. Saatavilla: http://resources.alcatel-lucent.com/?cid=194915